METODYKA AUDYTU WEWNĘTRZNEGO

§ 1

CYKLICZNOŚĆ

1. Zgodnie z Polską Normą PN-ISO/IEC 27001:2014-12 „Organizacja powinna ustanowić, wdrożyć, utrzymywać i ciągle doskonalić System Zarządzania Bezpieczeństwem Informacji (...)". [1]

2. Audyt wewnętrzny w zakresie Systemu Zarządzania Bezpieczeństwem Informacji powinien być prowadzony cyklicznie, co w praktyce oznacza roczne odstępy czasu pomiędzy jednym, a drugim audytem. Cykliczność w zakresie wykonywania czynności audytowych jest konieczna, by można było ocenić, czy System Zarządzania Bezpieczeństwem Informacji (SZBI) został skutecznie wdrożony. [2]

§ 2

PLAN AUDYTU

Zgodnie z Polską Normą PN-ISO/IEC 27001:2014-12: „Organizacja powinna:

1. zaplanować, ustanowić, wdrożyć i utrzymywać program (programy) audytów, w tym częstość audytów, metody, odpowiedzialność, wymagania dotyczące planowania oraz raportowanie. Program (programy) audytów powinien (powinny) uwzględniać znaczenie procesów objętych audytem oraz wyniki poprzednich audytów,

2. zdefiniować kryteria audytu i zakres każdego audytu,

3. wybierać audytorów i prowadzić audyty w sposób zapewniający obiektywność i bezstronność procesu audytu,

4. zapewnić przedstawienie wyników audytów właściwym członkom kierownictwa,

5. zachować udokumentowane informacje jako dowód realizacji programu (programów) audytów i wyników audytów." [3]

§ 3

AUDYTOR WEWNĘTRZNY / INSPEKTOR OCHRONY DANYCH

1. Działania audytowe w organizacji w zakresie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) wykonuje wyznaczony w sposób zgodny z obowiązującymi normami prawnymi Inspektor Ochrony Danych (IOD)

2. Jeśli Inspektor Ochrony Danych nie został wyznaczony w organizacji, instytucja nie jest zwolniona z podejmowania działań audytowych i w konsekwencji to Administrator Danych jest zobligowany do przeprowadzania audytów wewnętrznych. [4]

---

1 Norma PN-ISO/IEC 27001:2014-12, pkt 4.4
2 Norma PN-ISO/IEC 27001:2014-12, pkt 9.2
3 Norma PN-ISO/IEC 27001:2012-12, pkt 9.2
4 Norma PN-ISO/IEC 27001:2014-12, pkt 9.2

- formę i zakres relacji zawartych w umowach." [5]

β) Kontekst zewnętrzny: „środowisko wewnętrzne, w którym organizacja dąży do osiągnięcia swoich celów (...). Kontekst zewnętrzny może uwzględniać:

- środowisko kulturowe, społeczne, polityczne prawne, regulacyjne, finansowe, technologiczne, ekonomiczne, naturalne oraz konkurencyjne środowisko niezależnie od rozpatrywanego zakresu: międzynarodowego, narodowego, regionalnego lub lokalnego,
- kluczowe czynniki i trendy mające wpływ na cele organizacji, oraz
- relacje z zewnętrznymi interesariuszami, ich postrzeganie i wartości." [6]

3. Audytor wewnętrzny badający funkcjonowanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) powinien odwoływać się zarówno do kontekstu zewnętrznego jak i wewnętrznego organizacji, by wspomóc proces realizacji celów organizacji (uwzględniając cele bezpieczeństwa informacji) mając jednocześnie na względzie proces ciągłego doskonalenia jednostki.

4. Inspektor Ochrony Danych powinien mieć na względzie kontekst organizacji i dążyć do jego zrozumienia.

§ 5

ZASADY AUDYTOWANIA

1. W ramach procesu audytowania, Inspektor Ochrony Danych powinien stosować tzw. „kodeks dobrych praktyk audytora" tzn. zachować.:

a) rzetelność: oznacza wykonywanie audytów sumiennie stosując się do obowiązujących organizację aktów prawnych; wykonywanie pracy zachowując zasadę bezstronności w oparciu o kompetencję pozwalającą ocenić zachowanie audytowanego wskazującego na chęć wywierania wpływu na audytora,

b) uczciwość w zakresie przedstawiania wyników: oznacza zapewnienie zgodności stanu faktycznego ze stanem przedstawianym najwyższemu kierownictwu w ramach raportowania,

c) należytą staranność: powinna być adekwatna do ważności zadania uwzględniając zdolność rozeznania wszystkich procesów i sytuacji audytowych,

d) poufność: oznacza zapewnienie ochrony informacji powziętych podczas procesu audytowania,

e) niezależność: oznacza zachowanie bezstronności oraz obiektywizmu wobec wniosków z audytu; audytor powinien działać poza obszarem konfliktu interesów i wpływów,

f) podejście oparte na przeprowadzaniu postępowania dowodowego: oznacza wybieranie takiej metody audytowania, która

5 Norma PN-ISO/IEC 27005:2014-01, pkt 3.5

6 Norma PN-ISO/IEC 27005:2014-01, pkt 3.4

pozwoli na uzyskanie wiarygodnych oraz odtwarzalnych wniosków z audytu. [7]

§ 6

PROCES WDROŻENIA PLANU AUDYTU WEWNĘTRZNEGO

1. Inspektor Ochrony Danych powinien zakomunikować najwyższemu kierownictwu plan audytu wewnętrznego.

2. Inspektor Ochrony Danych określa cel, zakres oraz kryteria audytu.

3. Inspektor Ochrony Danych cyklicznie komunikuje najwyższemu kierownictwu o postępach w zakresie realizacji celów w ramach bezpieczeństwa informacji.

4. Inspektor Ochrony Danych w przypadku audytowania obszarów, które ze względu na swoją specyfikę wymagają wiedzy eksperckiej, wnioskuje do Administratora Danych o zapewnienie osób dysponujących wiedzą techniczną (np. Administrator Systemów Informatycznych w kontekście audytowania obszaru środowiska komputerowego). Ekspert techniczny wchodzi w skład zespołu audytowego.

5. Inspektor Ochrony Danych z należytą starannością dokumentuje proces audytowania oraz zapewnia właściwe przechowywanie zapisów z audytu.

6. Inspektor Ochrony Danych dokonuje wyboru metody audytowania tj:

   - pobieranie próbek,
   - wywiad,
   - obserwacja,
   - weryfikacja na poziomie formalnoprawnym. [8]

§ 7

USTALENIA Z AUDYTU

1. Inspektor Ochrony Danych w procesie audytowania, za pomocą karty audytu stanowiącej załącznik nr 2b do niniejszej metodyki, stwierdza, opierając się o zastany stan faktyczny:

   - zgodność,
   - niezgodność,
   - obszar do doskonalenia.

7 Norma PN-EN ISO 19011:2012, pkt 4

8 Norma PN-EN ISO 19011:2012, pkt 5.4.1 – 5.4.4; 6.4.6; załącznik B

2. Inspektor Ochrony Danych wraz z ekspertami technicznymi, o ile wchodzili w skład zespołu audytowego, przygotowuje wnioski z przeprowadzonego audytu.

3. Inspektor Ochrony Danych, za pomocą karty audytu, o której mowa w § 7 pkt 1 niniejszej metodyki, opracowuje dla organizacji działania korygujące (dot. obszarów do doskonalenia i niezgodności) przywracające stan faktyczny zgodny z prawem (zaleca się przeprowadzenie spotkania zamykającego z najwyższym kierownictwem).

4. Inspektor Ochrony Danych opracowuje rekomendacje w zakresie zaudytowanych obszarów przetwarzania danych osobowych oraz przedstawia je Administratorowi Danych (zaleca się przeprowadzenie spotkania zamykającego z najwyższym kierownictwem).

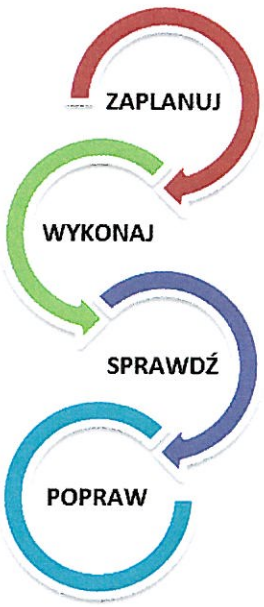
5. Złożenie na „ręce" Administratora Danych karty audytu oraz uzyskanie potwierdzenia (data wpływu/przyjęcia, pieczęć oraz podpis Administratora Danych) uznaje się za formalnoprawne przyjęcie treści raportu przez Administratora Danych. Poprzez to, Administrator Danych zobowiązany jest do zapewnienia środków technicznych i organizacyjnych Inspektorowi Ochrony Danych w celu minimalizacji zidentyfikowanego ryzyka utraty danych osobowych w wyniku nieprawidłowego postępowania organizacji w kontekście bezpieczeństwa informacji.

6. Działania korygujące oraz rekomendacje określone w ramach kart audytu, uznaje się za skrócony raport poaudytowy, którym Administrator Danych jest związany w taki sposób, iż powinien zareagować na stwierdzone przez Inspektora Ochrony Danych ryzyko.

7. Inspektor Ochrony Danych, w oparciu o wiedzę zebraną podczas audytowania, rewiduje obecnie obowiązujący w organizacji „kodeks dobrych praktyk" dostosowując go do aktualnej problematyki bezpieczeństwa informacji, z zachowaniem zgodności z wszystkimi normami prawnymi, do których to stosowania organizacja jest zobligowana.

8. **Inspektor Ochrony Danych wykonuje swoje obowiązki w oparciu o tzw. cykl Deminga (cykl PDCA), który to odnosi się ściśle do procesu ciągłego doskonalenia w ramach Systemu Zarządzania Bezpieczeństwem In formacji (SZBI) tj.:**

- **PLANOWANIE** (ang. **P**lan) – stworzenie planu audytu w oparciu o cele strategiczne organizacji oraz cele wyznaczone w ramach Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
- **WYKONANIE** (ang. **D**o) – określenie działań strategicznych, jakie Administrator Bezpieczeństwa Informacji będzie wykonywał w ramach realizowanego planu,
- **SPRAWDZENIE** (ang. **C**heck) – stwierdzenie zgodności / niezgodności / obszarów do doskonalenia w ramach audytowanych obszarów,
- **POPRAWIENIE / DZIAŁANIE** (ang. **A**ct) – określenie działań korygujących oraz rekomendacji w ramach audytowanych obszarów.



9. Inspektor Ochrony Danych w ramach realizowanych obowiązków powinien rozeznać następujące procesy:

OBSZARY BEZPIECZEŃSTWA INFORMACJI

- Środowisko komputerowe w tym programy ministerialne
- Bezpieczeństwo fizyczne
- Kontrola dostępu do zasobów
- Potrzeby stron zainteresowanych (kontekst zewnętrzny)
- Polityka Bezpieczeństwa jako zbiór procedur zapewniających zgodność formalnoprawną
- Organizacja wewnętrzna (kontekst wewnętrzny)
- Zasoby ludzkie (określenie roli i odpowiedzialności)
- Ocena ryzka jako kluczowy element zarządzania bezpieczeństwem informacji
- Zarządzanie aktywami
- Sprawna komunikacja (IOD ↔ ADO, IOD<->PRACOWNICY, ADO<->PRACOWNICY)

KARTA AUDYTU NR: 1

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
4.1 Kontekst organizacji A.5.1	Kierunek bezpieczeństwa informacji.	Zdolność organizacji do działania w ramach Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).	Sprawdzenie, czy podjęte do tej pory działania na rzecz bezpieczeństwa informacji są zgodne z normami prawnymi oraz regulacjami, w oparciu o które placówka działa. Weryfikacja przesłanek przetwarzania danych osobowych → weryfikacja sytuacji, w których organizacja pobiera zgodę na przetwarzanie danych osobowych → weryfikacja legalności przetwarzanych danych osobowych w ramach aktualnych procesów.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Dokumenty, które zawierają podpisaną klauzulę zgody na przetwarzanie danych osobowych.	Weryfikacja na poziomie formalnoprawnym. Działanie w oparciu o wywiad.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	W jednostce każdy pracownik przetwarza dane na mocy upoważnienia, które otrzymał od ADO. Pracownicy podpisali klauzule poufności. Jednostka działa w oparciu o przepisy prawa.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

20.12.2018r.

ADMINISTRATOR DANYCH (ADO):

O NUMERZE NIP:

ORAZ NUMERZE REGON

ADRES:

WÓJT GMINY AUGUSTÓW
ul. Mazurska 1 C
16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Administratora Bezpieczeństwa Informacji / Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **1** do **1**.

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Buksiński

24.10.2018

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych

KARTA AUDYTU NR: 2

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
4.2 Potrzeby stron zainteresowanych A.6.1	Organizacja wewnętrzna.	Bezpieczeństwo informacji w zakresie zarządzania projektami.	Analiza powierzenia danych osobowych oraz podpowierzenia danych osobowych w ramach realizowanych projektów.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Dokumentacja projektowa pn. „Energia odnawialna dla mieszkańców gminy Augustów”	Weryfikacja na poziomie formalnoprawnym. Działanie w oparciu o wywiad.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
Zgodność	1. Niniejszy projekt zawiera bazę danych osobowych dotyczących osób u których na ich nieruchomościach zostały zamontowane instalacje solarne. Wszyscy uczestnicy projektu podpisali klauzule informacyjna RODO. 2. Zawarto umowę powierzenia przetwarzania d.o. z Firmą Sanito sp z oo, ul. Puławska 476, 02-884 Warszawa 3. Umowa dotacji zawarta z Urzędem Marszałkowskim Woj. Podlaskiego zawiera postanowienia w zakresie powierzenia przetwarzania d.o.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

ADMINISTRATOR DANYCH (ADO):

O NUMERZE NIP:

WÓJT GMINY AUGUSTÓW
ul. Mazurska 1 C
16-300 Augustów

ORAZ NUMERZE REGON

ADRES:

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Administratora Bezpieczeństwa Informacji / Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **2** do **2**.

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Buksiński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 3

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
4.3 Zakres systemu zarządzania bezpieczeństwem informacji A.6.1 A.15.1	Relacje z podmiotami zewnętrznymi.	Bezpieczeństwo informacji w zakresie przekazywania danych osobowych podmiotom, które wykonują dla jednostki konkretne zadania (publiczne/zlecone/biznesowe).	Analiza aktualnie zawartych umów w zakresie współpracy jednostki z podmiotami, w ramach których zachodzi przesłanka determinująca konieczność podpisania umowy powierzenia danych osobowych. Określenie zasięgu przetwarzanych danych osobowych w ramach komunikacji zewnętrznej.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Przegląd umów o współpracy (macierzystych).	Metoda próbkowania. Działanie w oparciu o wywiad.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
Obszar do doskonalenia	Dokonano przeglądu wszystkich zawartych umów od 2018r. Umowy są sporządzane zgodnie z przepisami .Każdy podmiot świadczący usługi na rzecz jednostki podpisał umowę powierzenia danych. Brakuje umów powierzenia do oprogramowania Firmy Bryk oraz umowy powierzenia z firmą Project-Consulting.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
Zawrzeć umowy powierzenia z Firmą Bryk oraz z firmą Project-Consulting.	

ADMINISTRATOR DANYCH (ADO):

O NUMERZE NIP: WÓJT GMINY AUGUSTÓW

ORAZ NUMERZE REGON ul. Mazurska 1 C

ADRES: 16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Administratora Bezpieczeństwa Informacji / Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **3** do **3** .

ADMINISTRATOR DANYCH

WÓJT

mgr inż. Zbigniew Buksiński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 4

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
4.4 Ciągłość systemu zarządzania bezpieczeństwem informacji A.5.1.1	Kierunek bezpieczeństwa informacji.	Polityka bezpieczeństwa i jej formalnoprawne wdrożenie w placówce.	Sprawdzenie, czy obecna Polityka Bezpieczeństwa Informacji została wdrożona zarządzeniem i funkcjonuje w placówce jako zatwierdzona przez najwyższe kierownictwo.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Zarządzenie wprowadzające Politykę Bezpieczeństwa.	Weryfikacja na poziomie formalnoprawnym.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	Politykę Bezpieczeństwa została wprowadzona zarządzeniem Nr KK.120.11.2018 Wójta Gminy Augustów z dnia 20 grudnia 2018r. w sprawie: wprowadzenia Polityki Bezpieczeństwa Informacji przez ADO. Pracownicy zapoznali się z treścią zarządzenia.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

04.10.2019.

ADMINISTRATOR DANYCH (ADO):	Wójt Gminy Augustów
O NUMERZE NIP:	846-15-95-610
ORAZ NUMERZE REGON	
ADRES:	ul. Mazurska 1C, 16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Administratora Bezpieczeństwa Informacji / Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **4** do **4**.

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Bukszyński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 5

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
5.1 Zaangażowanie przywództwa A.5.1	Kierunek bezpieczeństwa informacji.	Zapewnienie przez najwyższe kierownictwo działań na rzecz bezpieczeństwa informacji zgodnie z założonymi celami organizacji.	Sprawdzenie celów i zakresu określonych w Polityce Bezpieczeństwa Informacji względem celów i zadań realizowanych przez najwyższe kierownictwo.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Polityka bezpieczeństwa Informacji Dokument określający misję jednostki (statut, regulamin organizacyjny).	Weryfikacja na poziomie formalnoprawnym.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	ZGODNOŚĆ ZAŁOŻEŃ POLITYKI BEZPIECZEŃSTWA INFORMACJI Z REGULAMINEM ORGANIZACYJNYM.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

06.11.2019r.

ADMINISTRATOR DANYCH (ADO): _____

O NUMERZE NIP: _____

ORAZ NUMERZE REGON _____

ADRES: _____

WÓJT GMINY AUGUSTÓW
ul. Mazurska 1 C
16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Administratora Bezpieczeństwa Informacji / Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **5** do **5** .

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Buksiński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 6

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
5.2 Polityka organizacji A.8.2	Klasyfikacja informacji.	Weryfikacja procesów w rozumieniu zbiorów danych osobowych.	Sprawdzenie aktualności zbiorów danych osobowych względem obecnie przetwarzanych. Weryfikacja pozioma: struktura zbiorów danych osobowych (dane zwykłe/dane szczególne). Weryfikacja pionowa: nowe zbiory danych osobowych występujące w placówce. Weryfikacja systemowa: sposób przetwarzania danych osobowych (na I poziomie - tradycyjnie/w ramach narzędzi i baz programowych/na II poziomie – ministerialnym).

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Wykaz zbiorów danych osobowych z Polityki Bezpieczeństwa Informacji wraz z określeniem programów bazodanowych oraz struktury zbioru.	Przeprowadzenie wywiadu z pracownikami upoważnionymi do przetwarzania danych osobowych w celu weryfikacji pionowej, poziomej oraz systemowej.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	ZWERYFIKOWANO WSZYSTKIE ZBIORY DANYCH OSOBOWYCH W DNIACH 22-24 PAŹDZIERNIKA 2019R. ,WYKAZ ZBIORÓW JEST ODPOWIEDNIO ROZBUDOWANY .ZAWIERA ZBIORY ORAZ INFORMACJĘ O PROGRAMACH ZASTOSOWANYCH DO PRZETWARZANIA DANYCH W WERSJI ELEKTRONICZNEJ.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH

1. **PLAN AUDYTU:**

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
NIE DOTYCZY			NIE DOTYCZY

20.12.2018r.

ADMINISTRATOR DANYCH (ADO):

O NUMERZE NIP:

ORAZ NUMERZE REGON

ADRES:

WÓJT GMINY AUGUSTÓW
ul. Mazurska 1 C
16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Administratora Bezpieczeństwa Informacji / Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **6** do **6**.

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Buksiński

24.10.2018

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 7

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
5.3 Odpowiedzialność i uprawnienia A.6.1	Organizacja wewnętrzna.	Weryfikacja odpowiedzialności za proces bezpieczeństwa informacji.	Weryfikacja upoważnień do przetwarzania danych osobowych względem osób faktycznie przetwarzających dane osobowe na terenie placówki (stażyści/praktykanci/wolontariusze). Weryfikacja zakresu upoważnienia do przetwarzania danych osobowych względem obowiązków wynikających z zatrudnienia lub zakresu czynności.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Upoważnienie do przetwarzania danych osobowych. Ewidencja osób upoważnionych do przetwarzania danych osobowych. Zakres obowiązków/zakres czynności.	Weryfikacja na poziomie formalnoprawnym.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	W DNIACH 9 WRZESNIA 2019R. DO 24 PAŹDZIERNIKA 2019R. ZWERYFIKOWANO UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH. KAŻDA OSOBA PRZETWARZAJĄCA DANE W JEDNOSTCE POSIADA NADANE PRZEZ ADO UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

20.12.2018r.

ADMINISTRATOR DANYCH (ADO):

O NUMERZE NIP:

ORAZ NUMERZE REGON

ADRES:

WÓJT GMINY AUGUSTÓW
ul. Mazurska 1 C
16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Administratora Bezpieczeństwa Informacji / Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **7** do **7**.

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Buksinski

24.10.2018

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych

KARTA AUDYTU NR: 8

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
6.1 Ocena ryzyka oraz weryfikacja szans A.11 A.11.1 A.11.2	Bezpieczeństwo fizyczne oraz środowiskowe	Analiza szacowania ryzyka.	Opracowanie / wykorzystanie narzędzi / wdrożenie procesu szacowania ryzyka w oparciu o fizyczną ochronę danych osobowych oraz środowisko komputerowe.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Analiza Szacowania Ryzyka Karta audytu fizycznego.	Wykonanie analizy szacowania ryzyka. Wydzielenie obszarów bezpiecznych. Wydzielenie obszarów do doskonalenia.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	WDROŻONO MECHANIZMY, ZA POMOCĄ KTÓRYCH ODBYWA SIĘ SZACOWANIE RYZYKA . ZOSTAŁA PRZEPROWADZONA ANALIZA RYZYKA. RYZYKO JEST AKCEPTOWALNE. ZOSTAŁY WPROWADZONE DZIAŁANIA , KTÓRE MAJĄ NA CELU POPRAWIENIE JAKOŚCI/SKUTECZNOŚCI OCHRONY DANYCH OSOBOWYCH.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

06.11.2019r.

ADMINISTRATOR DANYCH (ADO): _____

O NUMERZE NIP: _____

WÓJT GMINY AUGUSTÓW
ul. Mazurska 1 C
16-300 Augustów

ORAZ NUMERZE REGON _____

ADRES: _____

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Administratora Bezpieczeństwa Informacji / Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **8** do **8**.

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Buksiński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 9

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
6.2 Cele w zakresie bezpieczeństwa informacji A.5.1	Kierunek bezpieczeństwa informacji.	Cele w zakresie bezpieczeństwa informacji.	Weryfikacja aktywów niezbędnych do realizacji celów w zakresie bezpieczeństwa informacji, wytyczonych w porozumieniu z najwyższym kierownictwem. Określenie odpowiedzialności, zasobów, czasookresu realizacji wyznaczonych celów oraz mierników poziomu realizacji założonych planów.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Polityka rachunkowości organizacji.	Zaplanowanie środków finansowych na realizację celów ustalonych przez Administratora Danych wespół z Inspektorem Ochrony Danych.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	ZAPLANOWANO ŚRODKI FINANSOWE NA ZABEZPIECZENIE PROCESU BEZPIECZEŃSTWA INFORMACJ: - W ROKU 2019: KWOTA 1000 ZŁ NA ZAKUP CZYTNIKÓW RODO DO KSEROKOPIARKI KYOCERA, -NA 2020 R.: 10.100 ZŁ NA WYKONANIE AUDYTU ZGODNOŚCI Z KRI ORAZ OCHRONY D.O.; ZAKUP 3 SZT. KOMPUTERÓW -9.000 ZŁ.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

20.12.2018r.

ADMINISTRATOR DANYCH (ADO): _____

O NUMERZE NIP: _____

ORAZ NUMERZE REGON _____

ADRES: _____

WÓJT GMINY AUGUSTÓW
ul. Mazurska 1 C
16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **9** do **9**.

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew [illegible]

24.10.2018

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 10

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
7.1 Wsparcie w zakresie zasobów A.8.1	Odpowiedzialność za zasoby.	Identyfikacja zasobów organizacji.	Zidentyfikowanie aktywów, jakimi dysponuje organizacja oraz analiza potrzeb w zakresie dostępności innych zasobów, które usprawniłyby System Zarządzania Bezpieczeństwem Informacji (SZBI).

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Analiza szacowania ryzyka. Inwentaryzacja środków trwałych. Regulamin Wewnętrznych Procedur- Kodeks dobrych praktyk pracownika.	Zaplanowanie nabycia zasobów w formie usług lub środków trwałych np.: zakup nośników pamięci oraz stosowne ich zabezpieczenie; wdrożenie systemów wspomagających, zastosowanie kluczy kryptograficznych czy szaf metalowych.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	W RAMACH OBOWIAZUJĄCEGO KODEKSU DOBRYCH PRAKTYK,PRACOWNICY ZOSTALI ZOBLIGOWANI DO POSZERZANIA WIEDZY Z ZAKRESU PRZETWARZANIA I OCHRONY DANYCH OSOBOWYCH. KAŻDY PRACOWNIK WEDLE KODEKSU DBA O TO ABY PRZETWARZANE DANE ZOSTAŁY ODPOWIEDNIO ZABEZPIECZONE. ZESPÓŁ ADMINISTRACJI PROWADZI OPIS INWENTARZA,Z OBOWIĄZKOWYM NADANIEM NUMERÓW INWENTARZOWYCHNA WYPOSAŻENIU ORAZ EWIDENCJĘ AKTYWÓW.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

06.11.2019r.

ADMINISTRATOR DANYCH (ADO):

O NUMERZE NIP: WÓJT GMINY AUGUSTÓW

ORAZ NUMERZE REGON ul. Mazurska 1 C

ADRES: 16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **10** do **10** .

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Buksiński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 11

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
7.2 Kompetencja A.7.2	Zasób ludzki w kontekście realizowania obowiązków służbowych wynikających z zatrudnienia w organizacji.	Świadomość pracowników w zakresie obowiązków dotyczących Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).	Zorganizowanie i przeprowadzenie szkolenia z zakresu bezpieczeństwa informacji względem przetwarzanych danych osobowych w organizacji.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Zaświadczenia o ukończeniu szkolenia z zakresu ochrony danych osobowych. Lista obecności pracowników, którzy ukończyli szkolenie. Zakres merytoryczny i agenda przeprowadzonego szkolenia.	Nawiązanie współpracy z firmą zewnętrzną. Zbadanie wpływu przeprowadzonego szkolenia na realizację obowiązków pracowników uwzględniając problematykę ochrony danych osobowych.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	PRACOWNICY ZOSTALI PRZESZKOLENI Z ZAKRESU BEZPIECZEŃSTWA INFORMACJI I NOWYCH PRZEPISÓW RODO. ZASWIADCZENIA POTWIERDZAJĄCE UKONCZENIE SZKOLENIA W AKTACH OSOBOWYCH.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

20.12.2018r.

ADMINISTRATOR DANYCH (ADO): _____

O NUMERZE NIP: _____

ORAZ NUMERZE REGON _____

ADRES: _____

WÓJT GMINY AUGUSTOW
ul. Mazurska 1 C
16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **11** do **11** .

ADMINISTRATOR DANYCH

24.10.2018

WÓJT
mgr inż. Zbigniew Buksiński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 12

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
7.3 Świadomość A.7.2 A.16.1	Zasób ludzki w kontekście przetwarzanych danych osobowych w organizacji.	Świadomość pracowników w zakresie obowiązków dotyczących Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).	Zorganizowanie i przeprowadzenie szkolenia z zakresu bezpieczeństwa informacji względem przetwarzanych danych osobowych w organizacji.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Dziennik uchybień i zagrożeń Kodeks dobrych praktyk pracownika. Procedura Alarmowa	Opracowanie i wdrażanie kodeksu dobrych praktyk

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	PRACOWNICY ZOSTALI ZAPOZNANI Z KODEKSEM DOBRYCH PRAKTYK , JAK RÓWNIEŻ SĄ PRZESZKOLENI W ZAKRESIE ZGŁASZANIA INCYDENTÓW W JEDNOSTCE.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

ADMINISTRATOR DANYCH (ADO): _____

O NUMERZE NIP: _____

ORAZ NUMERZE REGON _____

ADRES: _____

WÓJT GMINY AUGUSTÓW
ul. Mazurska 1 C
16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **12** do **12** .

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Buksiński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 13

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
7.4 Komunikowanie się w organizacji A.7.2	Zasób ludzki w kontekście przetwarzanych danych osobowych w organizacji.	Polityka informacyjna Administratora Bezpieczeństwa Informacji.	Prowadzenie skutecznej polityki informacyjnej Inspektora Ochrony Danych względem pracowników przetwarzających dane osobowe w organizacji.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Plan spotkań IOD z pracownikami wraz ze wskazaniem następujących elementów: - treść komunikatu, - data spotkań i określenie częstotliwości spotkań, - lista osób wraz ze wskazaniem obecności obowiązkowej.	Opracowanie planu spotkań w ramach realizowania polityki informacyjnej IOD.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	INSPEKTOR OCHRONY DANYCH JEST W TRAKCIE OPRACOWYWANIA PLANU SPOTKAŃ . PLAN ZE WZGLĘDU NA WYSTĄPIENIE NIEPRZEWIDZIANE OKOLICZNIŚCI MOŻE ULEC ZMIANIE. PONADTO SPOTKANIA Z PRACOWNIKAMI REALIZWNAE SĄ NA BIEŻĄCO, W MIARĘ POTRZEB.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

20.12.2018r.

ADMINISTRATOR DANYCH (ADO):

O NUMERZE NIP: WÓJT GMINY AUGUSTÓW

ORAZ NUMERZE REGON ul. Mazurska 1 C

ADRES: 16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **13** do **13** .

ADMINISTRATOR DANYCH

WÓJT

mgr inż. Zbigniew Buksiński

24.10.2018

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 14

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
7.5 Dokumentacja procesowa A.11.1	Bezpieczeństwo fizyczne.	Procedury dot. archiwum/składnicy akt.	Weryfikacja: - procedur, - pomieszczeń.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Instrukcja kancelaryjna. Instrukcja archiwalna. Jednolity rzeczowy wykaz akt.	Weryfikacja na poziomie formalnoprawnym. Działanie w oparciu o obserwację. Działanie w oparciu o audyt fizycznej ochrony danych osobowych.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ /NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	PRACOWNICY POSTĘPUJĄ ZGODNIE Z PRZEPISAMI PRAWA W ZAKRESIE ZASAD KLASYFIKOWANIA I KWALIFIKOWANIA, UDOSTĘPNIANIA ORAZ PRZEKAZAYWANIA MATERIAŁÓW ARCHIWALNYCH DO ARCHIWÓW.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	BRAK

20.12.2018r.

ADMINISTRATOR DANYCH (ADO): _____

O NUMERZE NIP: _____

ORAZ NUMERZE REGON _____

ADRES: _____

WÓJT GMINY AUGUSTÓW
ul. Mazurska 1 C
16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **14** do **14** .

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Łuksiński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 15

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
8.1 Działania procesowo-operacyjne A.13.2	Procesy zlecone na zewnątrz.	Procedura nadzorowania procesów przetwarzania danych zleconych na zewnątrz.	Uzgodnienie procesu udostępniania danych osobowych innym podmiotom.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Wniosek o udostępnienie danych osobowych.	Metoda próbkowania . Metoda wywiadu. Zbadanie procedury udostępniania danych osobowych.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	PROCEDURA UDOSTĘPNIANIA DANYCH OSOBOWYCH ODBYWA SIĘ ZGODNIE Z PRZEPISAMI PRAWA .W JEDNOSTCE OBOWIĄZUJE ZAKAZ UDZIELANIA PRZEZ TELEFON INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

20.12.2018r.

ADMINISTRATOR DANYCH (ADO): _____

O NUMERZE NIP: _____ WÓJT GMINY AUGUSTÓW

ORAZ NUMERZE REGON _____ ul. Mazurska 1 C

ADRES: _____ 16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **15** do **15** .

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Łuksiński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 16

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
8.2 Ocena ryzyka A.16.1	Dokumentowa-nie procesu zarządzania ryzykiem.	Dowodzenie procesu audytowania.	Przechowywanie dokumentacji z zakresu szacowania ryzyka – gromadzenie materiału dowodowego.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Analiza Szacowania Ryzyka. Ocena ryzyka bezpieczeństwa informacji. Ocena ryzyka zawodowego.	Dochowanie należytej staranności w kontekście odpowiedniego przechowywania wyników z prowadzenia postępowania dowodowego w zakresie szacowania ryzyka.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	ORGANIZACJA PRZECHOWUJE WYNIKI SZACOWANIA RYZYKA.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

06.11.2019r.

ADMINISTRATOR DANYCH (ADO):

O NUMERZE NIP:

ORAZ NUMERZE REGON

ADRES:

WÓJT GMINY AUGUSTÓW
ul. Mazurska 1 C
16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **16** do **16** .

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Buksiński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych

KARTA AUDYTU NR: 17

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
8.3 Postępowanie z ryzykiem A.16.1	Postępowanie z ryzykiem.	Plan postępowania z ryzykiem.	Wdrożenie planu postępowania z ryzykiem: (działanie, tolerowanie, przeniesienie, wycofanie się).

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Analiza Szacowania Ryzyka. Ocena ryzyka bezpieczeństwa informacji. Plan postępowania z ryzykiem.	Stworzenie planu postepowania z ryzykiem.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	WDROŻONO ANALIZĘ SZACOWANIA RYZYKA W OPARCIU O RODO PLAN POSTĘPOWANIA Z RYZKIEM JEST W TRAKCIE OPRACOWY-WANIA.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

06.11.2019r.

ADMINISTRATOR DANYCH (ADO): _____

O NUMERZE NIP: _____

ORAZ NUMERZE REGON WÓJT GMINY AUGUSTÓW

ADRES: ul. Mazurska 1 C
16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

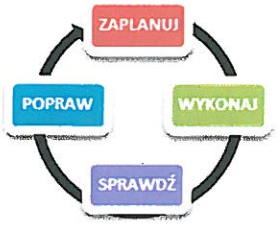
potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **17** do **17**.

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Buksiński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)



KARTA AUDYTU NR: 18

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
9.1 Monitoring wyników A.14.2	Proces monitorowania.	Zapewnienie bezpieczeństwa w procesach poprzez ciągłe monitorowanie skuteczności Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).	Stworzenie mechanizmów pozwalających na monitorowanie skuteczności Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Analiza Szacowania Ryzyka. Ocena ryzyka bezpieczeństwa informacji.	Określenie: - co należy monitorować, - co należy mierzyć, - metod monitorowania, - czasookresy monitorowania, - narzędzia służące do monitorowania wyników skuteczności procesu bezpieczeństwa informacji. Należy wziąć pod uwagę najsłabsze elementy np. Administrator Danych nie ustanawia zasad prac nad rozwojem oprogramowania, co zgodnie z oceną Inspektora Ochrony Danych miałoby swoje uzasadnienie.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	IODO MONITORUJE SYSTEM BEZPIECZEŃSTWA INFORMACJI . PROGRAMY NA BIEŻĄCO SĄ AKTUALIZOWANE. IODO STOSUJE SIĘ DO INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

06.11.2019r..

ADMINISTRATOR DANYCH (ADO): _____

O NUMERZE NIP: _____

ORAZ NUMERZE REGON _____

ADRES: _____

WÓJT GMINY AUGUSTÓW
ul. Mazurska 1 C
16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **18** do **18** .

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Buksiński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 19

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
9.2 Procedura audytów wewnętrznych A.16.1	Harmonogram audytowania.	Procedura audytów wewnętrznych.	Analiza i ocena wyników uprzednio przeprowadzonych audytów wewnętrznych – zastosowanie skali porównawczej.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Dokumentacja audytowa poprzedzająca aktualny plan audytu.	Weryfikacja na poziomie formalnoprawnym.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	IODO PROWADZI AKTUALNY PLAN AUDYTU.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

06.11.2019r.

ADMINISTRATOR DANYCH (ADO): _____

O NUMERZE NIP: _____

ORAZ NUMERZE REGON _____

ADRES: _____

WÓJT GMINY AUGUSTÓW
ul. Mazurska 1 C
16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **19** do **19** .

ADMINISTRATOR DANYCH

WÓJT
mgr Zbigniew Buksiński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 20

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
9.3 Przegląd zarządzania A.18.2	Przegląd Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).	Procedura przeglądu zarządzania.	Analiza i ocena wyników uprzednio przeprowadzonych procedur przeglądu zarządzania – zastosowanie skali porównawczej.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Procedura przeglądu zarządzania poprzedzająca aktualną procedurę.	Opracowanie procedury przeglądu zarządzania.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	JEDNOSTKA POSIADA OPRACOWANĄ I PRZYJĘTĄ DO STOSOWANIA INSTRIKCJĘ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM . IODO PROWADZI ANALIZĘ I OCENĘ WYNIKÓW UPRZEDNIO PRZEPROWADZONYCH PROCEDUR PRZEGLĄDU ZARZĄDZANIA.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

06.11.2019r..

ADMINISTRATOR DANYCH (ADO): _____

O NUMERZE NIP: _____

ORAZ NUMERZE REGON _____

ADRES: _____

WÓJT GMINY AUGUSTÓW
ul. Mazurska 1 C
16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **20** do **20** .

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Bukśiński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 21

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
10.1 Niezgodność A.18.1 A.18.2	Działania korygujące.	Badanie niezgodności.	Notyfikacja niezgodności w celu objęcia jej nadzorem. Skorygowanie oraz postępowanie z następstwami.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Karta ~~zgodności~~/niezgodności/~~obszarów do doskonalenia~~.	Zweryfikowanie procesów w celu ustalenia obszarów do doskonalenia. Opracowanie działań korygujących i przedstawienie ich Administratorowi Danych.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	JEŚLI W PLACÓWCE DOJDZIE DO NARUSZENIA, IODO SPORZĄDZA KARTĘ NIEZGODNOŚCI I PODEJMUJE DALSZE DZIAŁANIA NAPRAWCZE.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

06.11.2019r..

ADMINISTRATOR DANYCH (ADO): _____

O NUMERZE NIP: _____

WÓJT GMINY AUGUSTÓW
ul. Mazurska 1 C
16-300 Augustów

ORAZ NUMERZE REGON _____

ADRES: _____

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **21** do **21** .

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Baksiński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 22

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
10.2 Proces doskonalenia	Ciągłość w zakresie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).	Przydatność, adekwatność oraz skuteczność Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).	Wdrożenie ciągłości bezpieczeństwa informacji w sposób formalnoprawny poprzez dokumentowanie procesów, procedur, zabezpieczeń w celu zapewnienia funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w momentach kryzysu czy katastrofy.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Raport poaudytowy uwzględniający działania korygujące	Przekazanie Administratorowi Danych raportu poaudytowego wraz z propozycją wprowadzenia działań korygujących dla niezgodności. Monitorowanie i weryfikowanie wdrożonych zabezpieczeń mających zapewnić ciągłość bezpieczeństwa informacji.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	IOD PRZEWIDUJE SPORZĄDZENIE RAPORTU POAUDYTOWEGO KTÓREGO CELEM BĘDZIE WPROWADZENIE EWENTUALNYCH DZIAŁAŃ KORYGUJ ACYCH MAJĄC ZA ZADANIE ZMNIEJSZENIE RYZYKA ZWI,AZANEGO Z BEZPIECZEŃSTWEM PRZETWARZANIA DANYCH OSOBOWYCH.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

06.11.2019r.

ADMINISTRATOR DANYCH (ADO): _____

O NUMERZE NIP: WÓJT GMINY AUGUSTÓW _____

ORAZ NUMERZE REGON ul. Mazurska 1 C _____

ADRES: 16-300 Augustów _____

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **22** do **22** .

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Buksiński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

KARTA AUDYTU NR: 22

1. PLAN AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ
10.2 Proces doskonalenia	Ciągłość w zakresie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).	Przydatność, adekwatność oraz skuteczność Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).	Wdrożenie ciągłości bezpieczeństwa informacji w sposób formalnoprawny poprzez dokumentowanie procesów, procedur, zabezpieczeń w celu zapewnienia funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w momentach kryzysu czy katastrofy.

2. WYKONANIE:

DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
Raport poaudytowy uwzględniający działania korygujące	Przekazanie Administratorowi Danych raportu poaudytowego wraz z propozycją wprowadzenia działań korygujących dla niezgodności. Monitorowanie i weryfikowanie wdrożonych zabezpieczeń mających zapewnić ciągłość bezpieczeństwa informacji.

3. STWIERDZENIE ZGODNOŚCI/NIEZGODNOŚCI/OBSZARÓW DO DOSKONALENIA:

ZGODNOŚĆ/NIEZGODNOŚĆ/OBSZAR DO DOSKONALENIA	OPIS STANU FAKTYCZNEGO
ZGODNOŚĆ	IOD PRZEWIDUJE SPORZĄDZENIE RAPORTU POAUDYTOWEGO KTÓREGO CELEM BĘDZIE WPROWADZENIE EWENTUALNYCH DZIAŁAŃ KORYGUJ ACYCH MAJĄC ZA ZADANIE ZMNIEJSZENIE RYZYKA ZWI,AZANEGO Z BEZPIECZEŃSTWEM PRZETWARZANIA DANYCH OSOBOWYCH.

4. WPROWADZENIE DZIAŁAŃ KORYGUJĄCYCH:

DZIAŁANIA KORYGUJĄCE	REKOMENDACJE (ZALECENIA) INSPEKTORA OCHRONY DANYCH
NIE DOTYCZY	NIE DOTYCZY

06.11.2019r.

ADMINISTRATOR DANYCH (ADO): _____

O NUMERZE NIP: WÓJT GMINY AUGUSTÓW

ORAZ NUMERZE REGON ul. Mazurska 1 C

ADRES: 16-300 Augustów

DOTYCZY: Wynik audytu wewnętrznego z uwzględnieniem działań korygujących i rekomendacji

W oparciu o:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
  - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
  - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowe normy ISO:
  - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
  - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
  - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania),

potwierdzam, iż zapoznałem się z wynikiem audytu wewnętrznego w ramach działań Inspektora ochrony Danych Osobowych, zawartym w następujących dokumentach:

- metodyka audytu wewnętrznego,
- plan czynności audytowych,
- karty audytowe nr od **22** do **22** .

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Buksiński

(data przyjęcia do wiadomości, pieczęć oraz podpis Administratora Danych)

PLAN AUDYTU

CZASOOKRES AUDYTU: 20.12.2018 – 20.12.2019

PODMIOT AUDYTOWANY: URZĄD GMINY AUGUSTÓW

AUDYT PRZEPROWADZIŁ/A: ul. Mazurska 1 C
16-300 Augustów

CELE AUDYTU:

ZADANIA PUBLICZNE / CELE BIZNESOWE
Doprecyzowanie odpowiedzialności w zakresie procesu przetwarzania danych osobowych (w ramach informacji przetwarzanych wewnątrz oraz na zewnątrz organizacji)
Sprawna polityka informacyjna względem pracowników w kontekście zachowania zasad bezpieczeństwa informacji zgodnie z procedurami obowiązującymi w organizacji
Wspieranie organizacji w ramach zapewnienia bezpieczeństwa w procesach rozwoju oraz wsparcia
Dostosowanie zabezpieczeń organizacji do wymogów związanych z bezpieczeństwem systemów informacyjnych
Zapewnienie bezpieczeństwa fizycznego i środowiskowego
Zapewnienie procesu szkoleniowego skierowanego do osób przetwarzających dane osobowe w organizacji

KRYTERIA AUDYTU:

PODSTAWA PRAWNA
Kryterium wiodące: Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000)
Kryterium pomocnicze: PN-ISO/IEC 27001:2014-12
Kryterium pomocnicze: PN-EN ISO 19011:2012
Kryterium pomocnicze: PN-ISO/IEC 27005:2014-01

ZAKRES AUDYTU:

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ	DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
4.1 Kontekst organizacji A.5.1	Kierunek bezpieczeństwa informacji.	Zdolność organizacji do działania w ramach Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).	Sprawdzenie, czy podjęte do tej pory działania na rzecz bezpieczeństwa informacji są zgodne z normami prawnymi oraz regulacjami, w oparciu o które placówka działa. Weryfikacja przesłanek przetwarzania danych osobowych → weryfikacja sytuacji, w których organizacja pobiera zgodę na przetwarzanie danych osobowych → weryfikacja legalności przetwarzanych danych osobowych w ramach aktualnych procesów.	Dokumenty, które zawierają podpisaną klauzulę zgody na przetwarzanie danych osobowych.	Weryfikacja na poziomie formalnoprawnym. Działanie w oparciu o wywiad.
4.2 Potrzeby stron zainteresowanych A.6.1	Organizacja wewnętrzna.	Bezpieczeństwo informacji w zakresie zarządzania projektami.	Analiza powierzenia danych osobowych oraz podpowierzenia danych osobowych w ramach realizowanych projektów.	Dokumentacja projektowa.	Weryfikacja na poziomie formalnoprawnym. Działanie w oparciu o wywiad.
4.3 Zakres systemu zarządzania bezpieczeństwem informacji A.6.1 A.15.1	Relacje z podmiotami zewnętrznymi.	Bezpieczeństwo informacji w zakresie przekazywania danych osobowych podmiotom, które wykonują dla jednostki konkretne zadania (publiczne / zlecone / biznesowe).	Analiza aktualnie zawartych umów w zakresie współpracy jednostki z podmiotami, w ramach których zachodzi przesłanka determinująca konieczność podpisania umowy powierzenia danych osobowych. Określenie zasięgu przetwarzanych danych osobowych w ramach komunikacji zewnętrznej.	Przegląd umów o współpracy (macierzystych).	Metoda próbkowania. Działanie w oparciu o wywiad.
4.4 Ciągłość systemu zarządzania bezpieczeństwem informacji A.5.1.1	Kierunek bezpieczeństwa informacji.	Polityka bezpieczeństwa Informacji i jej formalnoprawne wdrożenie w placówce.	Sprawdzenie, czy obecna Polityka Bezpieczeństwa Informacji została wdrożona zarządzeniem i funkcjonuje w placówce jako zatwierdzona przez najwyższe kierownictwo.	Zarządzenie wprowadzające Politykę Bezpieczeństwa Informacji.	Weryfikacja na poziomie formalnoprawnym.
5.1 Zaangażowanie przywództwa A.5.1	Kierunek bezpieczeństwa informacji.	Zapewnienie przez najwyższe kierownictwo działań na rzecz bezpieczeństwa informacji zgodnie z założonymi celami organizacji.	Sprawdzenie celów i zakresu określonych w Polityce Bezpieczeństwa Informacji względem celów i zadań realizowanych przez najwyższe kierownictwo.	Polityka bezpieczeństwa Informacji Kontrola zarządcza: - plan działalności, - regulamin kontroli zarządczej. Dokument określający misję jednostki (statut, regulaminy organizacyjne, plan działalności).	Weryfikacja na poziomie formalnoprawnym.
5.2 Polityka organizacji A.8.2	Klasyfikacja informacji.	Weryfikacja procesów w rozumieniu zbiorów danych osobowych.	Sprawdzenie aktualności zbiorów danych osobowych względem obecnie przetwarzanych. Weryfikacja pozioma: struktura zbiorów danych osobowych (dane zwykłe/dane szczególne). Weryfikacja pionowa: nowe zbiory danych osobowych występujące w placówce. Weryfikacja systemowa: sposób przetwarzania danych osobowych (na I poziomie - tradycyjnie/w ramach narzędzi i baz programowych/na II poziomie – ministerialnym).	Wykaz zbiorów danych osobowych z Polityki Bezpieczeństwa Informacji wraz z określeniem programów bazodanowych oraz struktury zbioru.	Przeprowadzenie wywiadu z pracownikami upoważnionymi do przetwarzania danych osobowych w celu weryfikacji pionowej, poziomej oraz systemowej.

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ	DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
5.3 Odpowiedzialność i uprawnienia A.6.1	Organizacja wewnętrzna.	Weryfikacja odpowiedzialności za proces bezpieczeństwa informacji.	Weryfikacja upoważnień do przetwarzania danych osobowych względem osób faktycznie przetwarzających dane osobowe na terenie placówki (stażyści/praktykanci/wolontariusze). Weryfikacja zakresu upoważnienia do przetwarzania danych osobowych względem obowiązków wynikających z zatrudnienia lub zakresu czynności.	Upoważnienie do przetwarzania danych osobowych. Ewidencja osób upoważnionych do przetwarzania danych osobowych. Zakres obowiązków/zakres czynności.	Weryfikacja na poziomie formalnoprawnym.
6.1 Ocena ryzyka oraz weryfikacja szans A.11 A.11.1 A.11.2	Bezpieczeństwo fizyczne oraz środowiskowe.	Analiza szacowania ryzyka.	Opracowanie / wykorzystanie narzędzi / wdrożenie procesu szacowania ryzyka w oparciu o fizyczną ochronę danych osobowych oraz środowisko komputerowe.	Analiza Szacowania Ryzyka Ocena ryzyka. Karta audytu fizycznego.	Wykonanie analizy szacowania ryzyka. Wydzielenie obszarów bezpiecznych. Wydzielenie obszarów do doskonalenia.
6.2 Cele w zakresie bezpieczeństwa informacji A.5.1	Kierunek bezpieczeństwa informacji.	Cele w zakresie bezpieczeństwa informacji.	Weryfikacja aktywów niezbędnych do realizacji celów w zakresie bezpieczeństwa informacji, wytyczonych w porozumieniu z najwyższym kierownictwem. Określenie odpowiedzialności, zasobów, czasookresu realizacji wyznaczonych celów oraz mierników poziomu realizacji założonych planów.	Kontrola zarządcza. Polityka rachunkowości organizacji.	Zaplanowanie środków finansowych na realizację celów ustalonych przez Administratora Danych wespół z Inspektorem Ochrony Danych.
7.1 Wsparcie w zakresie zasobów A.8.1	Odpowiedzialność za zasoby.	Identyfikacja zasobów organizacji.	Zidentyfikowanie aktywów, jakimi dysponuje organizacja oraz analiza potrzeb w zakresie dostępności innych zasobów, które usprawniłyby System Zarządzania Bezpieczeństwem Informacji (SZBI).	Analiza szacowania ryzyka. Inwentaryzacja środków trwałych. Kodeks dobrych praktyk pracownika.	Zaplanowanie nabycia zasobów w formie usług lub środków trwałych np.: zakup nośników pamięci oraz stosowne ich zabezpieczenie; wdrożenie systemów wspomagających, zastosowanie kluczy kryptograficznych czy szaf metalowych.
7.2 Kompetencja A.7.2	Zasób ludzki w kontekście realizowania obowiązków służbowych wynikających z zatrudnienia w organizacji.	Świadomość pracowników w zakresie obowiązków dotyczących Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).	Zorganizowanie i przeprowadzenie szkolenia z zakresu bezpieczeństwa informacji względem przetwarzanych danych osobowych w organizacji.	Zaświadczenia o ukończeniu szkolenia z zakresu ochrony danych osobowych. Lista obecności pracowników, którzy ukończyli szkolenie. Kodeks dobrych praktyk pracownika. Zakres merytoryczny i legenda przeprowadzonego szkolenia.	Nawiązanie współpracy z firmą zewnętrzną. Przeanalizowanie złożonych ofert pod względem zakresu merytorycznego. Wybranie oferty. Zbadanie wpływu przeprowadzonego szkolenia na realizację obowiązków pracowników uwzględniając problematykę ochrony danych osobowych.
7.3 Świadomość A.7.2 A.16.1	Zasób ludzki w kontekście przetwarzanych danych osobowych w organizacji.	Świadomość pracowników w zakresie konsekwencji niestosowania się do wymogów Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).	Zapoznanie pracowników z procedurą notyfikowania uchybień i zagrożeń w kontekście bezpieczeństwa informacji. Zobowiązanie pracowników do zgłaszania naruszeń incydentów w zakresie bezpieczeństwa informacji oraz słabości związanych z bezpieczeństwem informacji (termin 72 godzin).	Kodeks dobrych praktyk pracownika przetwarzającego dane osobowe. Regulamin wewnętrznych procedur .	Opracowanie i wdrażanie kodeksu dobrych praktyk.

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ	DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
7.4 Komunikowanie się w organizacji A.7.2	Zasób ludzki w kontekście przetwarzanych danych osobowych w organizacji.	Polityka informacyjna Inspektora Ochrony Danych.	Prowadzenie skutecznej polityki informacyjnej Inspektora Ochrony Danych względem pracowników przetwarzających dane osobowe w organizacji.	Plan spotkań IOD z pracownikami wraz ze wskazaniem następujących elementów: - treść komunikatu, - data spotkań i określenie częstotliwości spotkań, - lista osób wraz ze wskazaniem obecności obowiązkowej.	Opracowanie planu spotkań w ramach realizowania polityki informacyjnej Inspektora Ochrony Danych.
7.5 Dokumentacja procesowa A.11.1	Bezpieczeństwo fizyczne.	Procedury dot. archiwum/składnicy akt.	Weryfikacja: - procedur, - pomieszczeń.	Instrukcja kancelaryjna. Instrukcja archiwalna. Jednolity Rzeczowy Wykaz Akt.	Weryfikacja na poziomie formalnoprawnym. Działanie w oparciu o obserwację. Działanie w oparciu o audyt fizycznej ochrony danych osobowych.
8.1 Działania procesowo-operacyjne A.13.2	Procesy zlecone na zewnątrz.	Procedura nadzorowania procesów przetwarzania danych zleconych na zewnątrz.	Uzgodnienie procesu udostępniania danych osobowych innym podmiotom.	Wniosek o udostępnienie danych osobowych.	Metoda próbkowania. Metoda wywiadu. Zbadanie procedury udostępniania danych osobowych. Stworzenie wniosku o udostępnienie danych osobowych.
8.2 Ocena ryzyka A.16.1	Dokumentowanie procesu zarządzania ryzykiem.	Dowodzenie procesu audytowania.	Przechowywanie dokumentacji z zakresu szacowania ryzyka – gromadzenie materiału dowodowego.	Analiza Szacowania Ryzyka. Ocena ryzyka bezpieczeństwa informacji. Ocena ryzyka zawodowego.	Dochowanie należytej staranności w kontekście odpowiedniego przechowywania wyników z prowadzenia postępowania dowodowego w zakresie szacowania ryzyka
8.3 Postępowanie z ryzykiem A.16.1	Postępowanie z ryzykiem.	Plan postępowania z ryzykiem.	Wdrożenie planu postępowania z ryzykiem (działanie, tolerowanie, przeniesienie, wycofanie się).	Analiza Szacowania Ryzyka Ocena ryzyka bezpieczeństwa informacji. Plan postępowania z ryzykiem.	Stworzenie planu postępowania z ryzykiem.

PUNKT NORMY PN-ISO/IEC 27001:2014-12	AUDYTOWANY OBSZAR	ZAKRES AUDYTU	PODJĘTA CZYNNOŚĆ	DOKUMENT O CHARAKTERZE STRATEGICZNYM	DZIAŁANIE O CHARAKTERZE STRATEGICZNYM
9.1 Monitoring wyników A.14.2	Proces monitorowania.	Zapewnienie bezpieczeństwa w procesach poprzez ciągłe monitorowanie skuteczności Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).	Stworzenie mechanizmów pozwalających na monitorowanie skuteczności Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).	Analiza Szacowania Ryzyka Ocena ryzyka bezpieczeństwa informacji.	Określenie: - co należy monitorować, - co należy mierzyć, - metod monitorowania, - czasookresy monitorowania, - narzędzia służące do monitorowania wyników skuteczności procesu bezpieczeństwa informacji. Należy wziąć pod uwagę najsłabsze elementy np. Administrator Danych nie ustanawia zasad prac nad rozwojem oprogramowania, co zgodnie z oceną Inspektora Ochrony Danych miałoby swoje uzasadnienie.
9.2 Procedura audytów wewnętrznych A.16.1	Harmonogram audytowania.	Procedura audytów wewnętrznych.	Analiza i ocena wyników uprzednio przeprowadzonych audytów wewnętrznych – zastosowanie skali porównawczej.	Dokumentacja audytowa poprzedzająca aktualny plan audytu.	Weryfikacja na poziomie formalnoprawnym.
9.3 Przegląd zarządzania A.18.2	Przegląd Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).	Procedura przeglądu zarządzania.	Analiza i ocena wyników uprzednio przeprowadzonych procedur przeglądu zarządzania – zastosowanie skali porównawczej.	Procedura przeglądu zarządzania poprzedzająca aktualną procedurę.	Opracowanie procedury przeglądu zarządzania.
10.1 Niezgodność A.18.1 A.18.2	Działania korygujące.	Badanie niezgodności.	Notyfikacja niezgodności w celu objęcia jej nadzorem. Skorygowanie oraz postępowanie z następstwami.	Karta ~~zgodności~~/niezgodności/~~obszarów do doskonalenia~~ Raport poaudytowy.	Zweryfikowanie procesów w celu ustalenia obszarów do doskonalenia. Opracowanie raportu poaudytowego i przedstawienie go Administratorowi Danych.
10.2 Proces doskonalenia	Ciągłość w zakresie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).	Przydatność, adekwatność oraz skuteczność Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).	Wdrożenie ciągłości bezpieczeństwa informacji w sposób formalnoprawny poprzez dokumentowanie procesów, procedur, zabezpieczeń w celu zapewnienia funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w momentach kryzysu czy katastrofy.	Raport poaudytowy uwzględniający działania korygujące.	Przekazanie Administratorowi Danych raportu poaudytowego wraz z propozycją wprowadzenia działań korygujących dla niezgodności. Monitorowanie i weryfikowanie wdrożonych zabezpieczeń mających zapewnić ciągłość bezpieczeństwa informacji.

OZNACZENIE ORGANIZACJI, DLA KTÓREJ ZOSTAŁ PRZYGOTOWANY PLAN AUDYTU

URZĄD GMINY AUGUSTÓW
ul. Mazurska 1 C
16-300 Augustów

(PIECZĘĆ)

INSPEKTOR OCHRONY DANYCH

Z up. WÓJTA
mgr Elżbieta Pszczoła
Sekretarz Gminy

(DATA ZŁOŻENIA PLANU AUDYTU ORAZ PODPIS INSPEKTORA OCHRONY DANYCH)

ADMINISTRATOR DANYCH

WÓJT
mgr inż. Zbigniew Bukso

(DATA PRZYJĘCIA DO WIADOMOŚCI, PIECZĘĆ ORAZ PODPIS ADMINISTRATORA DANYCH)