**PROJEKT „CYBERBEZPIECZNY SAMORZĄD”**

Nazwa działania:

**„AKTUALIZACJA POLITYKI BEZPIECZEŃSTWA”**

**Opis i specyfikacja istotnych warunków zamówienia:**

* Należy dokonać przeglądu aktualnie obowiązującej Polityki Bezpieczeństwa (zwanej dalej PB) i dokonać korekt w odpowiednich obszarach tego dokumentu,
* PB musi zawierać spójny i precyzyjny zbiór procedur, na których Urząd opiera budowę wewnętrznych danych, dokumentów i zasobów informatycznych, a także zarządza nimi. Precyzuje także, które z nich i w jaki sposób mają być chronione,
* Wstęp do PB powinien zawierać określenie, czym ona jest dla Urzędu i w jakim celu PB zostaje wdrożona,
* PB powinna zawierać określenie terminologii używanej w dokumencie oraz definicje pojęć,
* PB powinna zawierać ponadto w szczególności podane niżej elementy:
- określenie zakresu systemu bezpieczeństwa informacji,
- określenie zasobu informacyjnego,
- informację na temat ochrony danych osobowych (Urząd posiada Politykę Bezpieczeństwa Przetwarzania Danych Osobowych, należy ją przejrzeć i ewentualnie skorygować),
- informację o ochronie danych niejawnych (Urząd posiada regulacje wewnętrzne w tej sprawie),
- zasady organizacji bezpieczeństwa informacji w Urzędzie (Urząd posiada między innymi załączniki nr 1 i 2 do aktualnej PB opisujące odpowiednio: Zasady przeprowadzania szkoleń oraz Procedury zabezpieczania informacji w sposób uniemożliwiający nieuprawnionemu ich ujawnienie, modyfikację, usunięcie lub zniszczenie, załączniki te należy przejrzeć i ewentualnie skorygować),
- zasady współpracy ze stronami zainteresowanymi (zewnętrznymi),
- krótkie określenie polityki kontroli dostępu do informacji,
- opis zasad nadawania uprawnień, ich zmiany i odbierania (Urząd posiada taki opis w formie załącznika nr 3 do aktualnej PB, należy go przejrzeć i ewentualnie skorygować),
- klasyfikację informacji,
- określenie podstawowych zasad bezpieczeństwa informacji,
- krótki opis zarządzania aktywami i ryzykami (**w punkcie tym należy umieścić odniesienie do dokumentu pt.: Metodyki i Procedury Analizy Ryzyka , opracowanie tego dokumentu będzie uruchomione w odrębnym postępowaniu**),
- informację o autoryzacji nowych urządzeń (informacje te zawarte są częściowo w załączniku nr 6 do aktualnej PB, należy go przejrzeć i ewentualnie skorygować),
- informację o zarządzaniu systemami i sieciami,
- procedurę zarządzania incydentami bezpieczeństwa informacji
- procedurę zgłaszania incydentów cyberbezpieczeństwa do NASK
- określenie standardów bezpieczeństwa fizycznego, sprzętu i infrastruktury technicznej,
- informację o pracy na urządzeniach mobilnych oraz pracy na odległość (Urząd posiada taki opis w formie załącznika nr 7 do aktualnej PB, należy go przejrzeć i ewentualnie skorygować),
- informację o zarządzaniu zmianami,
- określenie planu ciągłości działania (**w punkcie tym należy umieścić odniesienie do dokumentu pt.: Plan Ciągłości Działania Systemów Informatycznych, opracowanie tego dokumentu będzie uruchomione w odrębnym postępowaniu**),
- krótkie określenie polityki wymiany informacji pomiędzy Urzędem a gminnymi jednostkami organizacyjnymi,
- informację o zapewnieniu zgodności z wymaganiami prawnymi i regulacyjnymi,
- procedurę określającą przeprowadzenie audytu w zakresie bezpieczeństwa informacji,
- procedurę przeglądu i aktualizacji zapisów PB,
- powołanie się na ogólnie obowiązujące przepisy prawa w zakresie nieuregulowanym przez PB (zestawienie tych przepisów)