POLITYKA BEZPIECZEŃSTWA INFORMACJI W RELACJACH Z DOSTAWCAMI PUBLICZNA SZKOŁA PODSTAWOWA IM. JANA ANTONIEGO GRABOWSKIEGO

Odniesienia – norma ISO/IEC 27001:2022: *A.1.5.19, A.1.5.20 A.1.5.22*

METRYKA DOKUMENTU	
Polityka Bezpieczeństwa Informacji w Relacjach z Dostawcami	
Opracował:	
Zweryfikował:	
Zatwierdził:	

REJESTR ZMIAN

Numer wydania	Data Wydania	Miejsce i opis zmiany

§1

Wprowadzenie

1. Niniejsza Polityka reguluje kwestie związane z bezpieczeństwem informacji w relacjach z dostawcami, oraz kwestie monitorowania, przeglądu i zarządzani zmianami w usługach świadczonych przez dostawców w Publicznej Szkole Podstawowej im. Jana Antoniego Grabowskiego.
2. Zasady bezpieczeństwa informacji obowiązują wszystkich kontrahentów, którzy w trakcie realizacji umowy otrzymują dostęp do zasobów informacyjnych Organizacji.

§2

Bezpieczeństwo Informacji w relacjach z dostawcami

1. Przed podjęciem decyzji o nawiązaniu współpracy z zewnętrznym dostawcą usług dotyczących infrastruktury dokonywana jest ocena kontrahenta pod kątem jego rzetelności i kompetencji (z uwzględnieniem np. posiadanych przez dany podmiot referencji, zakresu świadczonych usług, informacji o dotychczasowych klientach i liczby dotychczasowych oraz okresu przez jaki usługodawca funkcjonuje na rynku).
2. Zakres świadczonych usług oraz sposób ich realizacji powinien być możliwie precyzyjnie określony i wynikać powinien z zawartej umowy.
3. Wszelkie prace i działania usługodawcy na terenie Organizacji lub w jej systemie Informatycznym realizowane są pod nadzorem pracowników Szkoły Podstawowej.
4. Umowy zawierane z usługodawcami usług zewnętrznych powinny uwzględniać m.in. możliwość kontroli działalności zewnętrznych dostawców przez Organizację, zakres informacji i dokumentacji przekazywanych przez usługodawcę w związku ze świadczonymi usługami, zasady dotyczące obsługi zgłaszanych problemów w zakresie świadczonych usług.
5. Dostęp do infrastruktury teleinformatycznej ograniczony jest tylko do tych jej komponentów i w takim zakresie oraz czasie, jaki niezbędny jest do wykonania danej usługi, w szczególności z uwzględnieniem zasady ograniczenia dostępu do danych podlegających ochronie (w tym danych osobowych).
6. Osoby wykonujące czynności w celu wykonania umowy powinny być imienne wskazane przez Usługodawcę.
7. Dostęp do danych podlegających ochronie (w szczególności danych osobowych) umożliwiany jest w sytuacji i zakresie niezbędnym dla wykonania danej usługi.
8. Wymagane jest, aby w sytuacjach dostępu do informacji podlegających ochronie o czym mowa w ust. 7 powyżej, usługodawca oraz działające w jego imieniu osoby podlegały odpowiednim restrykcjom i zobowiązaniom dot. poufności i ochrony w zakresie adekwatnym do rodzaju danych do jakich ma dostęp.
9. Zapisy odnoszące się do zawierania umów powierzenia przetwarzania danych oraz weryfikacji podmiotów przetwarzających dane osobowe określają obowiązujące w Organizacji zapisy dotyczące zawierania umów powierzenia przetwarzania danych osobowych.
10. Przy doborze zewnętrznych usługodawców usług informatycznych – zwłaszcza w przypadku usług o kluczowym znaczeniu dla Organizacji uwzględniane jest ryzyko związane z danymi usługami i obejmuje oceną sytuację ekonomiczno-finansową usługodawcy, zapewnianego przez niego poziomu bezpieczeństwa oraz jakości świadczonych usług w miarę możliwości również na podstawie doświadczeń innych podmiotów, które korzystały z usług dostawców.

§3

Uwzględnianie bezpieczeństwa informacji w relacjach z dostawcami

1. Przy opracowywaniu projektów umów, negocjacji umów z kontrahentem, Najwyższe Kierownictwo Organizacji w porozumieniu z Pełnomocnikiem SZBI identyfikuje wymagania bezpieczeństwa w odniesieniu do systemów informacyjnych Organizacji.
2. W odniesieniu do kontrahenta oraz nabywanych produktów lub usług, należy wziąć pod uwagę:
    1) zasady kontroli dostępu do systemów IT, w tym:
        a) dozwolone metody dostępu oraz kontroli,
        b) autoryzację praw dostępu i przywilejów dla użytkownika,

   c) prowadzenie listy osób uprawnionych do korzystania z udostępnianych usług wraz z ich prawami i przywilejami w odniesieniu do każdej z nich,
   d) przyznawanie, zmiana i odbieranie praw dostępu lub przerywania połączeń między systemami,
   e) przyjęcie zasady, że dostęp jest zabroniony, jeśli nie został jawnie przyznany,
2) poziom ochrony zasobów, w tym:
   a) poufność, integralność, dostępność oraz inne właściwości zasobów, istotne dla danej umowy,
   b) ograniczenie kopiowania i ujawniania informacji,
   c) korzystanie z zapisów o zachowaniu poufności,
   d) wymagane zabezpieczenia i mechanizmy ochrony fizycznej,
   e) ochronę przed złośliwym oprogramowaniem,
   f) zapewnianie zwrotu lub niszczenia zasobów w chwili zakończenia umowy lub w innym uzgodnionym w umowie czasie,
3) powiadamianie, raportowanie i śledzenie zdarzeń związanych z naruszeniem bezpieczeństwa informacji lub ciągłości działania,
4) prawo do monitorowania i blokowania działań związanych z zasobami informacyjnymi Organizacji,
5) nadzór realizacji umowy, oczekiwany oraz nieakceptowany poziom usług,
6) wymagania dla ciągłości usług, w tym pomiaru ich dostępności i niezawodności,
7) weryfikowalne kryteria wydajności, sposób ich monitorowania i raportowania,
8) strukturę i zakres raportowania oraz formy raportów,
9) zarządzanie zmianami oraz wymagania dotyczące instalowania i utrzymywania oprogramowania/sprzętu,
10) prawo do przeprowadzenia audytów określonych w umowie,
11) ustalenie zakresu audytów, ewentualnego zlecania tych czynności stronie trzeciej,
12) zabezpieczenia, jakie kontrahent ma wdrożyć u siebie lub u poddostawców, jeśli tacy występują, odpowiedzialność wynikającą z przepisów prawa oraz odpowiedzialność finansową,
13) prawo do własności intelektualnej i praw autorskich,
14) szkolenie pracowników Szkoły Podstawowej lub kontrahenta, z którymi są zawarte umowy,

§4

Monitorowanie, przegląd i zarządzanie zmianami w usługach dostawców

1. Organizacja monitoruje jakość usług świadczonych przez dostawców zewnętrznych, a wszystkie istotne spostrzeżenia wynikające z tego monitoringu są prezentowane Najwyższemu Kierownictwu.
2. Zakres, częstotliwość i metody monitorowania i raportowania powinny uwzględniać specyfikę świadczonych usług oraz ich istotność z perspektywy ciągłości i bezpieczeństwa działania Organizacji.
3. Organizacja sprawuje kontrolę nad działalnością usługodawcy w zakresie świadczonych przez niego usług. Kontrola taka może w szczególności polegać na weryfikacji stosowanych przez dostawcę mechanizmów kontrolnych lub przeglądzie wyników weryfikacji mechanizmów kontrolnych realizowanych przez audyt wewnętrzny usługodawcy lub niezależnych audytorów zewnętrznych. Informacje w tym zakresie są prezentowane Najwyższemu Kierownictwu.
4. Relacja biznesowa z każdym usługodawcą w zakresie usług informatycznych jest zarządzana po stronie Organizacji przez ASI. Osoba ta jest odpowiedzialna za relacje z danym usługodawcą, w tym za zamieszczenie odpowiednich zapisów w umowie za weryfikowanie jakości usług i za raportowanie wyników oceny jakości usług oraz wszystkich innych istotnych kwestii.
5. Każdy system informatyczny dostarczany przez zewnętrznego dostawcę usług ma swojego właściciela, przypisanego zgodnie z niniejszą Polityką.