Wielkopolski Związek Strzelectwa Sportowego

61 – 361 Poznań, ul. Starołęcka 36
tel./fax – 61 895 08 05, e-mail: biuro@wzss.pl
NIP: 779 21 45 389 / REGON: 634158061 konto bankowe – 26 1090 1362 0000 0001 3617 8402
Związek wpisany do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej prowadzonego przez Sąd Rejonowy Poznań Nowe Miasto i Wilda w Poznaniu – Wydział VIII Gospodarczy - Krajowego Rejestru Sądowego pod numerem **0000093230.**

OCENA
zgodności postępowania z danymi osobowymi w Wielkopolskim Związku Strzelectwa Sportowego (zwanym dalej **„WZSS”**) **z Normą Europejską EN ISO/IEC 27002:2017**

Dokonuje się niniejszym oceny zgodności postępowania z danymi osobowymi w WZSS z **Normą Europejską EN ISO/IEC 27002:2017 Information technology – Security techniques – Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)** mającą status Polskiej Normy. Na podstawie uwzględnienia w/w Normy formułuje się następujące **wnioski:**

1) **w zakresie organizacji bezpieczeństwa informacji:**

a) urządzenia mobilne i telepraca:

i. w WZSS operuje się urządzeniami mobilnymi przyjętymi na wyposażenie WZSS,
ii. ogranicza się w urządzeniach mobilnych instalację oprogramowania, innego niż konieczne do wykonywania czynności w WZSS zgodnie z przedmiotem jego działalności,
iii. urządzenia mobilne WZSS posiadają na bieżąco aktualizowane oprogramowanie zapewniające bezpieczeństwo ochrony danych osobowych oraz kompatybilność z oprogramowaniem wykorzystywanym przez partnerów WZSS,
iv. urządzenia mobilne WZSS nie uzyskują dostępu do sieci publicznych, lecz korzystają z własnego zasobu sieciowego,
v. dostęp do urządzeń mobilnych WZSS zapewniony jest wyłącznie osobom wykonującym czynności w WZSS i ograniczony poprzez stosowanie hasła zabezpieczającego lub numeru PIN lub odcisku linii papilarnych,
vi. wykonuje się kopie zapasowe danych zgromadzonych na urządzeniach mobilnych WZSS z częstotliwością nie mniejszą niż raz w miesiącu,
vii. praca zdalna w WZSS może być wykonywana jedynie w warunkach zapewniających ciągłość dostępu do zabezpieczonej sieci, w godzinach zapewniających bezpośredni kontakt z osobami zarządzającymi działalnością WZSS, zdolnymi do podejmowania niezwłocznych działań w przypadku zagrożenia bezpieczeństwa ochrony danych,

2) **w zakresie bezpieczeństwa zasobów ludzkich:**

a) weryfikuje się kompetencje pracowników oraz współpracowników WZSS w zakresie ochrony danych osobowych i bezpieczeństwa informacji poprzez:

i. właściwy wywiad w trakcie rozmów kwalifikacyjnych,
ii. wgląd do certyfikatów, zaświadczeń, dyplomów,

b) zapoznaje się na bieżąco pracowników i współpracowników WZSS z obowiązującą w WZSS polityką ochrony danych osobowych,

c) informacje w zakresie obowiązków związanych z zapewnieniem bezpieczeństwa informacji i ochrony danych osobowych zamieszcza się w umowach o pracę oraz innych umowach cywilnoprawnych zawieranych przez WZSS z jego pracownikami i współpracownikami,

3) w zakresie zarządzania aktywami:

a) zapewnia się, by aktywa WZSS zawierające bazy danych bądź zbiory informacji, udostępniane pracownikom bądź współpracownikom WZSS były przekazywane z zachowaniem zasad bezpieczeństwa informacji,

4) w zakresie klasyfikacji informacji:

a) wprowadza się klasyfikację informacji na 4 (słownie: czterech poziomach):

i. **poziom A** – ujawnienie informacji nie powoduje żadnej szkody – dane powszechnie dostępne w domenie publicznej,
ii. **poziom B** – ujawnienie powoduje niewielki kłopot lub niewygodę w zakresie działalności – dane niedostępne w domenie publicznej, lecz niezawierające danych osobowych,
iii. **poziom C** – dane osobowe i inne dane, których ujawnienie ma nieznaczący i krótkoterminowy wpływ na działalność lub cele taktyczne,
iv. **poziom D** – dane osobowe, których ujawnienie ma poważny wpływ na długoterminowe cele strategiczne lub stwarza ryzyko dla przetrwania WZSS – dane osobowe bądź pozostałe dane, o których brak mowy w pkt i.-iii. powyżej,

5) w zakresie kontroli dostępu:

a) rozdziela się role związane z kontrolą dostępu w ten sposób, że następujące osoby zarządzające działalnością WZSS mają wyłączne uprawnienie do nadawania dostępu do informacji, tj. dokonują autoryzacji na podstawie wniosku i zarządzają dostępem – Prezes WZSS, Wiceprezesi WZSS, Sekretarz WZSS.
b) wprowadza się ogólną zasadę uzyskiwania dostępu: *Wszystko jest zabronione dopóki nie jest wyraźnie dozwolone,*
c) zapewnia się ciągłe monitorowanie korzystania z usług sieciowych stosowanych w WZSS,
d) odstępuje się od przydzielania pracownikom bądź współpracownikom WZSS jakichkolwiek praw uprzywilejowanego dostępu,
e) zapewnia się niezwłoczne pozbawienie dostępu w przypadku zagrożenia naruszenia danych przez osoby posiadające dostęp do danych wykorzystywanych w WZSS,
f) aplikacje i systemy wykorzystywane przez WZSS identyfikują zdarzenia związane z bezpieczeństwem, jeśli zostały wykryte potencjalne próby przełamywania zabezpieczeń logowania,
g) kontroluje się dostęp do kodów źródłowych programów oraz związanych z nimi elementów,

6) w zakresie bezpieczeństwa fizycznego i środowiskowego:

a) wyznacza się obszar bezpieczeństwa stanowiący siedzibę WZSS oraz wszystkie miejsca, w których WZSS wykonuje swoje statutowe zadania,
b) obszar bezpieczeństwa zabezpieczony jest przed dostępem osób trzecich (drzwi wejściowe wyposażone w system antywłamaniowy),

c) sprzęt WZSS ulokowany jest w taki sposób, by zminimalizować niepotrzebny dostęp do obszarów pracy; poza godzinami pracy komputery przenośne WZSS zamykane są w zabezpieczonej szafie / biurku,
d) okablowanie zasilające i telekomunikacyjne, przenoszące dane i wspomagające usługi informacyjne są chronione przed przechwyceniem, zakłóceniem lub uszkodzeniem,
e) sprzęt WZSS serwisowany jest wyłącznie przez autoryzowany personel,
f) dane i informacje zamieszczone na nośnikach danych wymagające zniszczenia usuwa się poprzez skasowanie lub nadpisanie informacji za pomocą technik uniemożliwiających ich odtworzenie,
g) nie pozostawia się sprzętu WZSS bez opieki,
h) z drukarek usuwa się niezwłocznie wrażliwe lub klasyfikowane informacje,
i) w pozostałym zakresie aktualna pozostaje Polityka Czystego Biurka i Ekranu WZSS,
j) zważywszy na dotychczasowy przebieg procesów w WZSS nie zachodzi potrzeba podejmowania szczególnych środków zarządzania pojemnością; w przypadku jednak zaistnienia w przyszłości problemu ograniczenia lub braku pojemności zapewnia się: usuwanie nieaktualnych danych (przestrzeń dysków twardych), deinstalację aplikacji, systemów, baz danych oraz środowisk oraz optymalizację procesów wsadowych i harmonogramów,
k) zabrania się w WZSS korzystania z nieautoryzowanego oprogramowania,
l) automatycznie uaktualnia się oprogramowanie do wykrywania oraz usuwania szkodliwego oprogramowania,
m) dokonuje się regularnego, automatycznego, w odstępach czasu nie rzadziej niż raz w tygodniu skanowania pod kątem zagrożenia szkodliwym oprogramowaniem:

   i. wszystkich plików odbieranych poprzez sieci lub na innych nośnikach pamięci,
   ii. załączników poczty elektronicznej,
   iii. sprawdza się nadto strony internetowe pod kątem obecności szkodliwego oprogramowania,

n) wykonuje się kopie zapasowe baz danych i informacji zgromadzonych na nośnikach WZSS z częstotliwością nie mniejszą niż raz w miesiącu;
o) zapewnia się procedurę automatycznego zapisu kopii zapasowych baz danych i informacji zgromadzonych na nośnikach WZSS,
p) zapewnia się stałe monitorowanie operacji dokonywanych w bazach danych WZSS poprzez kontrolowanie dzienników zdarzeń,
q) wszystkie zegary urządzeń WZSS podlegają synchronizacji z wykorzystaniem czasu odniesienia – serwerów czasu znajdujących się w Głównym Urzędzie Miar, w Laboratorium Czasu i Częstotliwości,
r) dopuszcza się audyt systemów informacyjnych przez niezależne, bezstronne podmioty, którym WZSS audyt ten powierzy, po uprzedniej weryfikacji, czy podmioty dokonujące audytu systemów są w stanie zachować poufność przeprowadzanych czynności,

7) w zakresie bezpieczeństwa komunikacji:

a) podłączenie systemów do sieci wymaga uwierzytelnienia,
b) umowy dotyczące usług sieciowych zawierają zidentyfikowane mechanizmy zabezpieczeń,
c) w przypadku potrzeby zapewnia się rozdzielenie w strukturze sieci grup usług informacyjnych, użytkowników i systemów informacyjnych,
d) nie pozostawia się wiadomości zawierających poufne informacje w automatycznych sekretarkach,

e) odstępuje się od korzystania z faksów,
f) nie przekazuje się informacji poufnych za pomocą powszechnie dostępnych aplikacji i komunikatorów sieciowych w tzw. mediach społecznościowych,

8) w zakresie pozyskiwania, rozwoju i utrzymywania systemów:

a) wymagania związane z bezpieczeństwem informacji w WZSS odzwierciedlają wartość odpowiednich informacji oraz potencjalne szkody dla działalności, które mogłyby być wynikiem braku odpowiednich zabezpieczeń,
b) zapewnia się chronienie informacji przesyłanych w sieciach publicznych, związanych z usługami świadczonymi przez aplikacje, przed nieuczciwymi działaniami, sporami dotyczącymi umów oraz nieuprawnionym ujawnieniem i zmianami,
c) informacje związane z transakcjami dokonywanymi w ramach usług świadczonych przez aplikacje są chronione, aby zapobiec przerwaniu transmisji, błędom w trasowaniu, nieuprawnionym zmianom wiadomości, nieuprawnionemu ujawnieniu, powieleniu lub odtworzeniu,
d) zmiany w oprogramowaniu następują tylko w sytuacji, gdy jest to niezbędne dla zapewnienia właściwego poziomu ochrony bezpieczeństwa informacji we wdrażanych bądź aktualizowanych przedsięwzięciach/projektach,
e) WZSS nadzoruje i monitoruje prace rozwojowe nad systemami zlecone podmiotom zewnętrznym,

9) w zakresie relacji z dostawcami:

a) WZSS identyfikuje i dokumentuje rodzaje dostawców: usług informatycznych, usług finansowych, informatycznych elementów infrastruktury teleinformatycznej,
b) WZSS dokonuje wyboru dostawców usług, biorąc w pierwszej kolejności pod uwagę ograniczenie dostępu dostawców do informacji przetwarzanych w WZSS, a także zachowanie integralności tych informacji,
c) WZSS dobiera dostawców usług z uwzględnieniem potrzeby zapewnienia ciągłości dostaw technologii informacyjnych i telekomunikacyjnych,
d) WZSS dąży do uzyskania uzasadnionego zaufania, że dostarczane produkty technologii informacyjnych i komunikacyjnych funkcjonują prawidłowo, bez żadnych nieprzewidzianych lub niepożądanych właściwości; w przeciwnym razie WZSS rozwiązuje umowy z dotychczasowymi dostawcami z zachowaniem potrzeby zachowania ciągłości dostaw i wybiera nowych dostawców,
e) dostawcy usług zobowiązani są zapewniać wsparcie WZSS w przypadku kryzysu dostaw w systemie całodobowym,
f) WZSS monitoruje poziom realizacji usług w celu sprawdzenia, czy umowy z dostawcami są właściwie realizowane,

10) w zakresie zarządzania incydentami związanymi z bezpieczeństwem informacji:

a) osobą odpowiedzialną za zarządzanie incydentami związanymi z bezpieczeństwem informacji w WZSS jest Prezes Zarządu, a w jego zastępstwie również Wiceprezesi Zarządu oraz Sekretarz,
b) w przypadku incydentu związanego z bezpieczeństwem informacji podejmuje się w pierwszej kolejności działania mające na celu minimalizację skutków związanych z zagrożeniem bezpieczeństwa informacji oraz przeciwdziałanie zagrożeniom w przyszłości,

c) w przypadku powstania szkody związanej z przetwarzaniem informacji w WZSS ustala się zakres tej szkody i powiadamia o niej osobę poszkodowaną oraz odpowiednie organy kontroli,
d) po każdym incydencie związanym z bezpieczeństwem informacji WZSS zabezpiecza się dowody procesowe,
e) każdy incydent związany z bezpieczeństwem informacji w WZSS podlega analizie pod kątem:

i. skuteczności zabezpieczeń,
ii. oczekiwanej integralności, poufności lub dostępności informacji,
iii. ewentualnych błędów ludzkich,
iv. zgodności działań z politykami WZSS i zaleceniami,
v. zgodności działań z obowiązującymi zabezpieczeniami fizycznymi,
vi. ewentualnych nienadzorowanych zmian systemu,
vii. ewentualnego niepoprawnego działania oprogramowania lub sprzętu,
viii. ewentualnego naruszenia zasad dostępu,

f) pracownicy i kontrahenci korzystający z systemów i usług informacyjnych WZSS są zobowiązani do zgłaszania zdarzeń związanych z bezpieczeństwem informacji,
g) w przypadku, gdy ocena incydentu związanego z bezpieczeństwem informacji w WZSS jest utrudniona, zleca się podmiotowi wyspecjalizowanemu przeprowadzenie analizy śledczej, mającej na celu wykrycie przyczyny, rozmiaru i skutków incydentu oraz osób odpowiedzialnych za jego zaistnienie, z uwzględnieniem zasad poufności,

11) w zakresie aspektów bezpieczeństwa informacji w zarządzaniu ciągłością działania:

a) w niekorzystnych sytuacjach wymagania w zakresie bezpieczeństwa informacji pozostają takie same jak te w naturalnych warunkach eksploatacyjnych,

12) w zakresie zgodności z wymaganiami prawnymi i umownymi:

a) zapewnia się zidentyfikowanie, udokumentowanie i aktualizowanie wszystkich istotnych wymagań prawnych, regulacyjnych, umownych oraz podejścia WZSS do ich przestrzegania,
b) zapewnia się zgodność działalności WZSS z wymaganiami prawnymi, regulacyjnymi
c) i umownymi, związanymi z prawem własności intelektualnej i użytkowaniem prawnie zastrzeżonego oprogramowania poprzez nabywanie licencji do użytkowania wyłącznie od uprawnionych właścicieli praw bądź ich autoryzowanych przedstawicieli.