**Załącznik nr 1 do zapytania ofertowego**

Zakres usług informatycznych:

1. Bieżące konsultacje w opracowywaniu planów strategicznych rozwoju w zakresie szeroko pojętego obszaru funkcjonowania MNP w zakresie informatyki.
2. Konsultacje technologiczne, ocena wymagań dotyczących planowania i realizacji projektów IT w Gmachu Głównym i Oddziałach Muzeum Narodowego w Poznaniu mających na celu m.in. rozbudowę infrastruktury IT .
3. Wsparcie w przeprowadzaniu procedury bezpiecznej utylizacji sprzętu komputerowego, zakończone przedłożeniem do zatwierdzenia właściwego Zastępcy Dyrektora Muzeum Narodowego w Poznaniu.
4. Wsparcie w przygotowywaniu procedur zakupowych z zakresu teleinformatyki.
5. Wsparcie i administracja w zakresie obsługi konfiguracji oraz działania technologii webowych wykorzystywanych w Muzeum Narodowym w Poznaniu, w szczególności: aktualizacje, badanie podatności, eliminacja podatności, zarządzanie stronami WWW, weryfikacja zgodności WCAG 2.1.
6. Aktualizacje systemów zarządzania treścią (CMS).
7. Wsparcie w zakresie obsługi BIPu MNP, pomoc przy obsłudze Epuap.
8. Bieżące wsparcie dla funkcjonowania poczty elektronicznej.
9. Zapewnienie prawidłowego funkcjonowania oraz użytkowania strefy DMZ oraz serwerów znajdujących się w tej strefie.
10. Bieżąca analiza i informowanie o stanie obszaru cyberbezpieczeństwa, bieżąca weryfikacja funkcjonowania i rekomendowanie dodatkowych koniecznych działań podejmowanych dla Muzeum Narodowego w Poznaniu w zakresie przygotowania i gotowości oraz realizacji wytycznych dotyczących działań antyterrorystycznych i ogłoszonych stopni alarmowych wpływających na odpowiednie funkcjonowanie Muzeum Narodowego w Poznaniu.
11. Stałe wsparcie i kontrola stanu bezpieczeństwa systemów IT.
12. Monitorowanie wdrażania systemów bezpieczeństwa, w tym firewall.
13. Identyfikacja potencjalnych podatności i luk w zabezpieczeniach systemów (Windows, Linux) działających w Muzeum Narodowego w Poznaniu.
14. Regularne informowanie o nowo powstałych podatnościach oraz ryzykach wycieku danych w systemach, urządzeniach, aplikacjach.
15. Aktualizacja, weryfikacja oraz przedstawianie rekomendacji z zakresu realizacji zaleceń, procedur i polityk bezpieczeństwa dotyczących strefy teleinformatycznej.
16. Udział w zarządzaniu ryzykiem z zakresu cyberbezpieczeństwa.
17. Proponowanie nowych rozwiązań w zakresie bezpieczeństwa systemów IT oraz pomoc przy ich wdrażaniu.
18. Współpraca z zewnętrznymi partnerami w obszarze wykonywania zadań.
19. Realizacja zadań we współpracy z ASI, Inspektorem Ochrony Danych oraz stanowiskiem ds. ryzyka.
20. Zapewnianie aktualnych materiałów szkoleniowych i szkolenia dla pracowników MNP (dopuszczalna forma szkolenia - aktualizowana prezentacja online) z zakresu cyberbezpieczeństwa.
21. Bieżące zapewnienie aktualnych materiałów szkoleniowych i odpowiedni instruktaż grupy pracowników, odpowiedzialnych za działanie systemów informatycznych w celu zapewnienia bezpieczeństwa w MNP z powyższego zakresu.
22. Opracowywanie planów reagowania na incydenty.
23. Bieżąca analiza adekwatności i wsparcie w doskonaleniu procedur bezpieczeństwa cybernetycznego i zarządzania incydentami.
24. W przypadku wystąpienia ataków cybernetycznych, hakerskich podjęcie po uzgodnieniu z wyznaczoną osobą w Muzeum Narodowym w Poznaniu natychmiastowego działania. Następnie sformułowanie rekomendacji dotyczących eliminacji ryzyka i wprowadzenia mechanizmów kontrolnych.
25. Analiza podatności systemów informatycznych działających w Muzeum Narodowym w Poznaniu, w tym przeprowadzanie okresowo testów penetracyjnych. Wskazanie rekomendacji dotyczących zabezpieczeń systemów IT.
26. Wsparcie z zakresu administracji sieciowej oraz systemowej zasobów Muzeum Narodowego w Poznaniu (aplikacji zainstalowanych na serwerach, eksploatacji systemów) .
27. Wsparcie w administracji usługami sieciowymi, systemowymi, wirtualizacjami i systemami bazodanowymi wykorzystywanymi w Muzeum Narodowym w Poznaniu, w szczególności: Windows serwer, Linux, Vmware, Hyper-V, Azure, Office365, relacyjne bazy danych, nierelacyjne bazy danych.
28. Wsparcie z zakresu zarządzania usługami, sieciami, podsieciami DNS VPN, DHCP w Muzeum Narodowym w Poznaniu i jego Oddziałach w tym w administrowaniu
	1. rozwiązaniami sieciowymi takimi jak: Cisco, Ubiquiti, Fortinet, BitDefender.
29. Wsparcie we wdrażaniu zaleceń i wytycznych po audytowych.
30. Rozwiązywanie problemów związanych z DNS, konfiguracja stref, przekierowań itp.
31. Monitorowanie obciążenia baz danych, przepustowości i czasu odpowiedzi.
32. Bieżące wsparcie w zakresie wykonywania kopii zapasowych i planów odzyskiwania danych.
33. Weryfikacja administrowania systemem backupu danych, stanu (jakości) posiadanych kopii zapasowych i cykliczne ich odtwarzanie na podstawie ustalonej z MNP próby, przynajmniej raz w miesiącu Wsparcie w archiwizacji danych znajdujących się na serwerach sieciowych, monitoring wykonywania archiwizacji, aktualizację i ustalanie częstotliwości tworzenia kopii bezpieczeństwa na serwerach, bibliotece taśmowej i taśmach.
34. Wsparcie w prawidłowej eksploatacji i administrowaniu serwerów oraz funkcjonowaniu mechanizmów uwierzytelnienia użytkowników, zgodnie z polityką bezpieczeństwa Muzeum Narodowego w Poznaniu.
35. Dbanie o bezpieczeństwo sieci oraz integralność i poufność danych (monitorowanie stanu klimatu w serwerowniach, ochrona przed wirusami i innym złośliwym oprogramowaniem) przez całą dobę (24 godziny) oraz reakcją na zagrożenia niezwłocznie po powzięciu informacji o ich wystąpieniu w tym współpracę w tej dziedzinie z odpowiednią komórką Muzeum Narodowego w Poznaniu.
36. Okresowe przeprowadzanie audytów bezpieczeństwa w celu identyfikacji potencjalnych luk w zabezpieczeniach na podstawie uzgodnionej próby.
37. Regularne monitorowanie wydajności serwerów i dostępności usług, cykliczna diagnostyka i identyfikacja problemów wydajnościowych sieci i systemów. Rekomendowanie rozwiązań mających na celu eliminację problemów wydajnościowych.
38. Cykliczne monitorowanie aktualności certyfikatów.
39. Comiesięczne przedkładanie raportu z przeprowadzonych prac w Muzeum Narodowym w Poznaniu.