Formularz: Ankieta weryfikacji dojrzałości pod kątem cyberbezpieczeństwa

Typ:

Rok: 2021

Dział 1. Ankieta.

W przypadku problemów technicznych (zapomniałam/łem hasła, nie widzę ankiety, coś nie działa w ankiecie) prosimy o zgłoszenia na adres statystyka@cez.gov.pl, lub pod numery telefonów 501 369 856, 501 370 599, 501 368 812, 501 369 795.

W przypadku problemów związanych z merytorycznym wypełnieniem ankiety prosimy o kontakt na adres csirt@cez.gov.pl .

<table>
<tr><td colspan="3">Ankieta weryfikacji dojrzałości pod kątem cyberbezpieczeństwa</td></tr>
<tr><td colspan="3">Dane podmiotu</td></tr>
<tr><td rowspan="2">Nazwa jednostki:
SP ZZOZ SZPITAL W IŁŻY</td><td rowspan="2">NIP:
7961704266</td><td>Kod świadczeniodawcy:
70001798</td></tr>
<tr><td>Numer księgi rejestrowej:
000000007211</td></tr>
<tr><td colspan="3">Pytania ankietowe</td></tr>
</table>

Zarządzanie (ZA)	Zespół odpowiedzialny za bezpieczeństwo (ZA.1)	W jednostce jest dedykowana osoba odpowiedzialna za ochronę danych osobowych (ZA.1.1)	001	TAK
		W jednostce jest dedykowana osoba odpowiedzialna za bezpieczeństwo fizyczne (Za.1.2)	002	TAK
		W jednostce jest dedykowana osoba odpowiedzialna za cyberbezpieczeństwo (ZA.1.3)	003	BRAK
		Osoby odpowiedzialne za cyberbezpieczeństwo, ochronę danych osobowych podlegają bezpośrednio pod kierownika jednostki (ZA.1.4)	004	TAK
	Działania zarządu jednostki (ZA.2)	Dyrektor jednostki odbył szkolenie w zakresie cyberbezpieczeństwa w ciągu ostatniego roku (ZA.2.1) Podać datę szkolenia w dolnej części	005	NIE Data:
		Dyrektor jednostki cyklicznie przegląda raport oceny ryzyka w jednostce (ZA.2.2)	006	TAK
		Dyrektor jednostki wydał zarządzenie o zintegrowanym systemie zarządzania bezpieczeństwem w jednostce (ZA.2.3)	007	TAK
		Dyrektor jednostki opublikował politykę bezpieczeństwa jednostki z uwzględnieniem cyberbezpieczeństwa (ZA.2.4)	008	TAK

Zarządzanie bezpieczeństwem informacji (SZBI)	Kroki podjęte w celu zapewnienia bezpieczeństwa informacji (SZBI.1)	SZBI.1.1 - konieczność zapewnienia bezpieczeństwa informacji jest ujęta w strategii informatyzacji jednostki	009	JEST
		SZBI.1.2 - zidentyfikowano cele bezpieczeństwa informacji, określono sposoby ich realizacji oraz przypisano odpowiedzialność za ich realizację	010	JEST
		SZBI.1.3 - działania w zakresie bezpieczeństwa informacji podjęto przed rokiem 2021	011	JEST
		SZBI.1.4 - jednostka opracowała i przyjęła kompleksową politykę bezpieczeństwa informacji (PBI)	012	JEST
		SZBI.1.5 - PBI opracowana w oparciu o właściwe standardy i dobre praktyki	013	JEST
		SZBI.1.6 - ostatni przegląd PBI jednostki przeprowadzono nie wcześniej niż rok temu	014	TAK
	Zarządzanie (SZBI.2) - Zasady, procedury i procesy zarządzania i monitorowania wymogów w zakresie regulacyjnym, prawnym, ryzyka, ochrony środowiska i operacyjnym w organizacji są zrozumiałe i informują o zarządzaniu ryzykiem cyberbezpieczeństwa	SZBI.2.1 - Polityka cyberbezpieczeństwa organizacji jest przekazywana pracownikom w toku okresowych szkoleń stanowiskowych	015	NIE MA
		SZBI.2.2 - zidentyfikowano kluczowe aktywa informacyjne (zbiory danych / systemy / usługi)	016	JEST
		SZBI.2.3 - aktywa zostały uwzględnione w rejestrze ryzyk jednostki	017	JEST
		SZBI.2.4 - Zarządzanie w organizacji oraz zarządzanie ryzykiem odnoszą się do zagrożeń związanych z cyberbezpieczeństwem	018	JEST
	Szacowanie ryzyka (SZBI.3) - Organizacja rozumie ryzyko cyberbezpieczeństwa dla działalności organizacyjnej (w tym misji, funkcji, wizerunku lub reputacji), zasobów organizacyjnych i osób	SZBI.3.1 - Podatności w zasobach są identyfikowane i dokumentowane	019	TAK
		SZBI.3.2 - w jednostce dokonuje się szacowania ryzyka związanego z zagrożeniami bezpieczeństwa informacji	020	TAK
		SZBI.3.3 - Zagrożenia, zarówno wewnętrzne, jak i zewnętrzne, są identyfikowane i dokumentowane	021	TAK
		SZBI.3.4 - Zagrożenia, podatności, prawdopodobieństwo wystąpienia i skutki są używane do określania ryzyka	022	TAK
		SZBI.3.5 - Odpowiedzi na ryzyko są identyfikowane i priorytetyzowane	023	TAK
	Strategia zarządzania ryzykiem (SZBI.4) - Priorytety, ograniczenia, tolerancja ryzyk i założenia organizacji są określone i wspierają decyzje dotyczące ryzyka operacyjnego	SZBI.4.1 - Procesy zarządzania ryzykiem są ustanawiane, zarządzane i uzgadniane z dyrektorem jednostki	024	TAK
		SZBI.4.2 - w organizacji wdrożono system oceny ryzyka	025	TAK
	Zarządzanie ryzykiem we współpracy zewnętrznej (SZBI.5) - Priorytety, ograniczenia, tolerancja ryzyk i założenia organizacji są określone i wykorzystywane do wspierania decyzji o ryzyku związanych z zarządzaniem ryzykiem łańcucha dostaw. Organizacja ustanowiła i wdrożyła procesy identyfikacji, szacowania i zarządzania ryzykiem łańcucha dostaw	SZBI.5.1 - Procesy zarządzania ryzykiem cyberbezpieczeństwa są identyfikowane, ustanawiane, oceniane	026	TAK
		SZBI.5.2 - Partnerzy zewnętrzni i dostawcy w zakresie systemów informacyjnych, komponentów i usług są identyfikowani, priorytetyzowani i oceniani za pomocą procesu oceny ryzyka cyberbezpieczeństwa	027	TAK
		SZBI.5.3 - Umowy z dostawcami i partnerami zewnętrznymi są wykorzystywane do wdrażania odpowiednich środków dla osiągnięcia celów programu cyberbezpieczeństwa	028	TAK
		SZBI.5.4 - Dostawcy i partnerzy zewnętrzni są stale oceniani przy użyciu audytów, wyników testów lub innych form oceny w celu potwierdzenia, że wywiązują się ze swoich zobowiązań w zakresie bezpieczeństwa	029	TAK

OCHRONA (OCH)	Zarządzanie tożsamościami, uwierzytelnianie i kontrola dostępu (OCH.1)	OCH.1.1 - W jednostce wdrożono system zarządzania tożsamością i uprawnieniami	030	TAK
		OCH.1.2 - Fizyczny dostęp do zasobów jest zarządzany i chroniony	031	TAK
		OCH.1.3 - Dostęp zdalny jest zarządzany	032	TAK
		OCH.1.4 - Uprawnienia dostępu i autoryzacja są zarządzane z uwzględnieniem zasady najniższych uprawnień i rozdzielenia obowiązków	033	TAK
		OCH.1.5 - Integralność sieci jest chroniona (np. poprzez segregację sieci czy jej segmentację)	034	TAK
		OCH.1.6 - weryfikacja dostępu opiera się o MFA (uwierzytelnianie wieloskładnikowe) i jest wykorzystywana aktualnie	035	NIE
	Świadomość i podnoszenie kompetencji (OCH.2)	OCH.2.1 - w jednostce wdrożono system zarządzania tożsamością i uprawnieniami	036	NIE
		OCH.2.2 - Użytkownicy ze zwiększonymi uprawnieniami rozumieją swoje role i obowiązki	037	TAK
		OCH.PK-3 - Podmioty zewnętrzne (np. dostawcy, klienci, partnerzy) rozumieją swoje role i obowiązki	038	TAK
		OCH.2.3 - Kadra kierownicza wyższego szczebla rozumie swoje role i obowiązki.	039	TAK
		OCH.2.4 - Personel cyberbezpieczeństwa oraz bezpieczeństwa fizycznego rozumie swoje role i obowiązki	040	TAK
	Bezpieczeństwo danych (OCH.3)	OCH.3.1 - Dane w spoczynku są chronione	041	TAK
		OCH.3.2 - Przesyłane dane są chronione	042	TAK
		OCH.3.3 - Zasoby są formalnie zarządzane podczas usuwania, przenoszenia i dysponowania	043	TAK
		OCH.3.4 - Utrzymywana jest odpowiednia zdolność do zapewnienia dostępności	044	TAK
		OCH.3.5 - Wdrożono mechanizmy ochrony przed wyciekami danych	045	TAK
	Bezpieczeństwo kopii zapasowych. Plany reagowania na zagrożenia (OCH.4)	OCH.4.1 - Kopie zapasowe informacji są sporządzane, utrzymywane i testowane	046	TAK
		OCH.4.2 - Dostęp do kopii zapasowych jest dodatkowo chroniony	047	TAK
		OCH.4.3 - Dane są niszczone zgodnie z funkcjonującymi politykami	048	TAK
		OCH.4.34- Opracowano plan backupu i odmiejscowienia kopii zapasowych	049	TAK
		OCH.4.5 - Organizacja posiada i zarządza planami reagowania (w zakresie reagowania na incydenty i ciągłości działania) oraz planami odtwarzania (w zakresie odtwarzania po incydencie i po awarii)	050	TAK
		OCH.4.6 - Plany reagowania i odtwarzania są weryfikowane i testowane	051	TAK
		OCH.4.7 - Opracowano i wdrożono plan zarządzania podatnościami	052	NIE
	Technologia ochronna (OCH.5)	OCH.TO-1 - Zapisy logów/inspekcji są określone, dokumentowane, wdrażane i sprawdzane zgodnie z politykami	053	NIE
		OCH.TO-2 - Nośniki wymienne są chronione, a ich stosowanie ograniczone zgodnie z politykami	054	TAK
		OCH.TO-3 - Zasada najmniejszej funkcjonalności jest wdrożona poprzez odpowiednią konfigurację systemów tak, by posiadały tylko niezbędne możliwości	055	TAK
		OCH.TO-4 - Łącza komunikacyjne do internetu są chronione.(AntyDDoS i inne)	056	TAK
		OCH.TO-5 - Odpowiednie mechanizmy (jak np. failsafe, równoważenie obciążenia, hot swap) są wdrażane w celu osiągnięcia wymagań dotyczących odporności w normalnych i niekorzystnych sytuacjach	057	NIE

Zdarzenia i monitoring(CM)	Anomalie i zdarzenia (CM.1)	CM.1.1 - Wykryte zdarzenia są analizowane aby zrozumieć cele i metody ataku	058	TAK
		CM.1.2- Dane o zdarzeniach są pozyskiwane oraz korelowane z wielu źródeł i czujników	059	TAK
	Ciągłe monitorowanie bezpieczeństwa (CM.2)	CM.2.1 - Sieć jest monitorowana w celu wykrywania potencjalnych zdarzeń cyberbezpieczeństwa. (SIEM)	060	TAK
		CM.2.2 - Środowisko fizyczne jest monitorowane w celu wykrycia potencjalnych zdarzeń cyberbezpieczeństwa	061	TAK
		CM.2.3 - Aktywność personelu jest monitorowana w celu wykrycia potencjalnych zdarzeń związanych z cyberbezpieczeństwem	062	TAK
		CM.2.4 - Złośliwy kod jest wykrywany	063	TAK
		CM.2.5 - Nieautoryzowany kod mobilny jest wykrywany (np. ActiveX, JavaScript)	064	NIE
		CM.2.6 - Aktywność zewnętrznego dostawcy usług jest monitorowana w celu wykrywania potencjalnych zdarzeń cyberbezpieczeństwa	065	TAK
		CM.2.7 - Przeprowadza się monitorowanie pod kątem nieautoryzowanego personelu, połączeń, urządzeń i oprogramowania	066	TAK
		CM.2.8 - Przeprowadza się skanowanie podatności	067	TAK
REAGOWANIE (RE)	Planowanie reagowania (RE)	RE.1 - Plan reagowania jest realizowany w trakcie lub po incydencie	068	TAK
	Komunikacja (KO)	KO.1 - Personel zna swoje role i kolejność operacji, na wypadek konieczności reagowania	069	TAK
		KO.2 - Incydenty są zgłaszane zgodnie z ustalonymi kryteriami	070	TAK
		KO.3 - Informacje są udostępniane zgodnie z planami reagowania	071	TAK
		KO.4 - Koordynacja z zainteresowanymi stronami jest prowadzona w sposób zgodny z planami reagowania	072	NIE
		KO.5 - Dobrowolna wymiana informacji z zewnętrznymi podmiotami jest prowadzona w celu osiągnięcia szerszej świadomości sytuacyjnej w zakresie cyberbezpieczeństwa	073	NIE
	Mitygacja (MI)	MI.1 - Incydenty są opanowywane	074	TAK
		MI.2 - Incydenty są mitygowane	075	TAK
		MI.3 - Nowo zidentyfikowane podatności są mitygowane lub dokumentuje się akceptację ryzyka związanego z nimi	076	TAK
	Udoskonalanie (UD)	UD.1 - Plany reagowania uwzględniają wyciągnięte wnioski	077	TAK
		UD.2 - Strategie reagowania są aktualizowane	078	TAK
ODTWARZANIE (OD)	Planowanie odtwarzania (OD.1)	OD.1.1 - Plan odtwarzania jest realizowany w trakcie lub po incydencie cyberbezpieczeństwa	079	TAK
	Aktualizacja (OD.2)	OD.2.1 - Plany odtwarzania zawierają wyciągnięte dotychczas wnioski	080	TAK
		OD.2.2 - Strategie odtwarzania są aktualizowane	081	TAK

INFRASTRUKTURA (IN)	Sieć LAN (IN.1)	IN.1.1 przełączniki klasy enterprise, wsparcie	082	TAK
		IN.1.2 segmentacja sieci	083	TAK
	Ochrona brzegowa (IN.2)	IN.2.1 Firewall klasy enterprise, aktualne wsparcie, aktualizacje na bieżąco	084	TAK
		IN.2.2 połączenia VPN oraz certyfikaty dla wszystkich użytkowników	085	TAK
	Poczta (IN.3)	IN.3.1 serwer poczty	086	NIE
		IN.3.2 wdrożony SANBOX	087	NIE
		IN.3.3 wdrożony MFA dla wszystkich użytkowników usług pocztowych i aktualnie wykorzystywany	088	NIE
	Wirtualizacja (IN.4)	IN.4.1 serwery wirtualne	089	TAK
		IN.4.2 wsparcie i aktualizacje	090	TAK
	Kopia zapasowa (IN.5)	IN.5.1 Kopia odmiejscowiona	091	TAK
		IN.5.2 Napęd taśmowy (biblioteka taśmowa)	092	NIE
		IN.5.3 System kopii zapasowej izolowany od środowisk produkcyjnych	093	TAK
	Systemy bezpieczeństwa (IN.6)	IN.6.1 SIEM	094	NIE
		IN.6.2 DLP	095	NIE
		IN.6.3 NAC	096	NIE
		IN.6.4 WAF	097	TAK
		IN.6.5 DAM	098	NIE
		IN.6.6 EDR	099	NIE
		IN.6.7 DNS Protection	100	TAK
		IN.6.8 IPS/IDS	101	NIE
		IN.6.9 Antyvirus	102	TAK
		IN.6.10 SOC	103	NIE
	Urządzenia specjalizowane (IN.7)	IN.7.1 Tomograf komputerowy	104	TAK
		IN.7.2 Urządzenia do rezonansu magnetycznego	105	TAK
		IN.7.3 Cyfrowe urządzenia RTG	106	TAK
		IN.7.4 Kardiomonitory	107	TAK
		IN.7.5 Andiografy	108	TAK
		IN.7.6 Pompy infuzyjne	109	TAK

Telekomunikacja	typ łącza telekomunikacyjnego	110	4)Dzierżawione miedziane asymetryczne (ADSL)
	przepustowość (w przypadku łącz niesymetrycznych suma download + upload)	111	6) od 10 do 99,9 Mbps
	Usługa AntyDDoS	112	JEST
	firewall dostarczony przez operatora i prze operatora zarządzany	113	JEST
	firmowe telefony komórkowe	114	TAK
	telefonia VoIP wewnątrz jednostki	115	JEST
	łącze głosowe	116	8) VOiP
	łącze głosowe awaryjne, niezależne od zasilania lokalnego	117	2) JEST - GSM
	centralka telefoniczna	118	7) stacjonarna PSTN
Zasilanie Awaryjne	UPS na stanowisku roboczym	119	na wybranych
	Wszystkie serwerownie zasilane z UPS w czasie rozruchu generatora	120	TAK
	Wszystkie serwery z zasilaczami redundantnymi	121	TAK
	Generator awaryjny na potrzeby wszystkich serwerowni i intensywnej terapii	122	TAK
	SZR załączający generator awaryjny w trakcie pracy na UPS	123	TAK
	Zatankowany zbiornik paliwa wystarczy na	124	2) 12 h do 24 h
	Zasilanie jednostki z dwóch stacji transformatorowych SN/NN	125	NIE WIEM
	Awaryjne zasilanie we wszystkich serwerowniach	126	TAK

Dyrektor
Samodzielnego Publicznego Zespołu
Zakładów Opieki Zdrowotnej - Szpital w Iłży
Joanna Pionka
/dokument podpisany kwalifikowanym
podpisem elektronicznym/