Cyberbezpieczny Samorząd

Informacje podstawowe	
Nazwa jednostki:	Gmina Lesznowola
TERYT:	1418032
Liczba pracowników zatrudniona w urzędzie JST (obecnie)	140
Liczba pracowników zatrudniona w urzędzie JST (po 2 latach od rozliczeniu grantu)	140
Liczba użytkowników systemów IT (obecnie)	140
Liczba użytkowników systemów IT (po 2 latach od rozliczeniu grantu)	140
Łączna liczba etatów przewidzianych do obsługi i utrzymania elementów systemu cyberbezpieczeństwa w JST	4
Przewidziany budżet JST na finansowanie obszaru cyberbezpieczeństwa (w bieżącym roku)	200000
Przewidziany budżet JST na finansowanie obszaru cyberbezpieczeństwa (w kolejnym roku po rozliczeniu grantu)	240000
Przewidziany budżet JST na finansowanie obszaru cyberbezpieczeństwa (po 2 latach od rozliczenia grantu)	290000

Powyżej proszę wprowadzać wartości liczbowe

Cyberbezpieczny Samorząd

Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego (i Jednostkach Podległych)

Obszar	Zagadnienie	Działanie	Stan obecny	Stan planowany	Opis planowanego zakresu zmian	Stan zrealizowany	Opis zrealizowanego zakresu zmian
Zarządzanie (ZA)	Zespół odpowiedzialny za bezpieczeństwo. (ZA.1)	W Jednostce jest dedykowana osoba odpowiedzialna za ochronę danych osobowych.	TAK	TAK			
		W Jednostce jest dedykowana osoba odpowiedzialna za bezpieczeństwo fizyczne.	NIE	NIE			
		W Jednostce jest dedykowana osoba odpowiedzialna za cyberbezpieczeństwo.	TAK	TAK			
		Osoby odpowiedzialne za cyberbezpieczeństwo, ochronę danych osobowych podlegają bezpośrednio pod Kierownika JST.	TAK	TAK			
	Działania zarządu Jednostki (ZA.2)	Kierownik JST odbył szkolenie w zakresie cyberbezpieczeństwa w ciągu ostatniego roku.	NIE	TAK	Zaplanowano szkolenie kadry kierowniczej.		
		Kierownik JST cyklicznie przegląda raport oceny ryzyka w Jednostce.	NIE	TAK	Zaplanowano cykliczny przegląd raportu oceny ryzyka przez Kierownika JST.		
		Kierownik JST wydał zarządzenie o zintegrowanym Systemie Zarządzania Bezpieczeństwem Informacji (SZBI) w Jednostce.	TAK	TAK			
		Kierownik JST opublikował Politykę Bezpieczeństwa Informacji (PBI) Jednostki z uwzględnieniem cyberbezpieczeństwa.	TAK	TAK	Aktualnie opracowano i wdrożono politykę ochrony danych osobowych. Zaplanowano aktualizację kompleksowego SZBI, który uwzględni ochronę wszystkich informacji chronionych prawnie, łącznie z obszarem cyberbezpieczeństwa.		
	Strategia wobec Centrum Usług Wspólnych (ZA.3)	Jednostka jest obsługiwana przez Centrum Usług Wspólnych (CUW) w zakresie zarządzania IT.	NIE	NIE			
		Jednostka jest obsługiwana przez Centrum Usług Wspólnych w zakresie bezpieczeństwa teleinformatycznego.	NIE	NIE			
		Jednostka jest obsługiwana przez Centrum Usług Wspólnych w zakresie ochrony danych osobowych.	NIE	NIE			
	(SZBI.1) Kroki podjęte w celu zapewnienia bezpieczeństwa informacji	Konieczność zapewnienia bezpieczeństwa informacji jest ujęta w strategii informatyzacji Jednostki.	NIE	NIE			
		Zidentyfikowano w Jednostce cele bezpieczeństwa informacji, określono sposoby ich realizacji oraz przypisano odpowiedzialność za ich realizację.	NIE	TAK	Zaplanowano aktualizację kompleksowego SZBI.		
		Jednostka opracowała i przyjęła kompleksową Politykę Bezpieczeństwa Informacji (PBI).	TAK	TAK	Zaplanowano kompleksową aktualizację PBI w ramach aktualizacji SZBI.		
		PBI Jednostki jest opracowana w oparciu o właściwe standardy i dobre praktyki.	TAK	TAK	Zaplanowano kompleksową aktualizację PBI w ramach aktualizacji SZBI.		

System Zarządzania Bezpieczeństwem Informacji (SZBI)		Ostatni przegląd PBI Jednostki przeprowadzono nie dawniej niż rok temu.	TAK	TAK	Zaplanowano kompleksową aktualizację PBI w ramach aktualizacji SZBI.		
	(SZBI.2) Zarządzanie. 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	Polityka Bezpieczeństwa Informacji w Jednostce jest ogólnie dostępna dla pracowników, a zmiany w niej są im komunikowane w toku okresowych szkoleń stanowiskowych.	TAK	TAK			
		Zidentyfikowano kluczowe aktywa informacyjne Jednostki (zbiory danych / systemy / usługi).	CZĘŚCIOWO	TAK	Zaplanowano aktualizację kompleksowego SZBI.		
		Aktywa Jednostki zostały uwzględnione w rejestrze ryzyk.	NIE	TAK	Zaplanowano wykonanie oceny ryzyka dla cyberbezpieczeństwa jednostki.		
		W Jednostce procesy zarządcze oraz zarządzanie ryzykiem odnoszą się do zagrożeń związanych z cyberbezpieczeństwem.	NIE	TAK	Zaplanowano wykonanie oceny ryzyka dla cyberbezpieczeństwa jednostki.		
	(SZBI.3) Szacowanie ryzyka. Organizacja rozumie ryzyko cyberbezpieczeństwa dla działalności organizacyjnej (w tym misji, funkcji, wizerunku lub reputacji), zasobów organizacyjnych i osób.	Podatności w zasobach Jednostki są identyfikowane i dokumentowane.	NIE	TAK	Zaplanowano wykonanie testów podatnościowych oraz opracowanie procedury zarządzania podatnościami w ramach SZBI.		
		W Jednostce dokonuje się szacowania ryzyka związanego z zagrożeniami bezpieczeństwa informacji.	TAK	TAK	Zaplanowano wykonanie oceny ryzyka dla cyberbezpieczeństwa jednostki.		
		W Jednostce zagrożenia wewnętrzne i zewnętrzne są identyfikowane i dokumentowane.	TAK	TAK	Zaplanowano opracowanie i wdrożenie SZBI, w tym politykę regulującą proces cyber threat intelligence.		
		Zagrożenia, podatności, prawdopodobieństwo ich wystąpienia i skutki są używane do określania ryzyka w Jednostce.	TAK	TAK	Zaplanowano wykonanie oceny ryzyka dla cyberbezpieczeństwa jednostki.		
		Odpowiedzi na ryzyka w Jednostce są identyfikowane i są im nadawane priorytety.	TAK	TAK	Zaplanowano wykonanie oceny ryzyka dla cyberbezpieczeństwa jednostki.		
	(SZBI.4) Strategia zarządzania ryzykiem. Priorytety, ograniczenia, tolerancja ryzyk i założenia organizacji są określone i wspierają decyzje dotyczące ryzyka operacyjnego.	Procesy zarządzania ryzykiem są ustanawiane, zarządzane i uzgadniane z Kierownikiem JST.	NIE	TAK	Procesy zarządzania ryzykiem zostaną ustanowione w ramach wdrożenie SZBI.		
		W Jednostce wdrożono system oceny ryzyka.	CZĘŚCIOWO	TAK	W ramach SZBI obecnie wykorzystywana metodologia zostanie rozszerzona o zagrożenia związne z cyberbezpieczeństwem.		

	(SZBI.5) Zarządzanie ryzykiem we współpracy zewnętrznej. 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.	Procesy zarządzania ryzykiem cyberbezpieczeństwa w Jednostce są identyfikowane, ustanawiane i oceniane.	CZĘŚCIOWO	TAK	Zaplanowano wykonanie oceny ryzyka oraz procedury zarzadzania ryzykiem dla cyberbezpieczeństwa jednostki.		
		Zewnętrzni partnerzy Jednostki i zewnętrzni dostawcy systemów informacyjnych, komponentów i usług są identyfikowani i oceniani za pomocą procesu oceny ryzyka cyberbezpieczeństwa.	CZĘŚCIOWO	TAK	Zaplanowano opracowanie polityki relacji z dostawcami oraz procedury zarządzania ryzykiem.		
		Umowy z zewnętrznymi dostawcami i partnerami zewnętrznymi Jednostki są wykorzystywane do wdrażania odpowiednich środków dla osiągnięcia celów programu cyberbezpieczeństwa.	CZĘŚCIOWO	TAK	W ramach wdrożenia SZBI zaplanowano opracowanie minimalnych klauzul umowanych dla umów serwisowych w ramach wdrożenia SZBI.		
		Zewnętrzni dostawcy i partnerzy zewnętrzni Jednostki są stale oceniani przy użyciu audytów, wyników testów lub innych form oceny w celu potwierdzenia, że wywiązują się ze swoich zobowiązań w zakresie bezpieczeństwa.	CZĘŚCIOWO	TAK	W ramach wdrożenia SZBI zaplanowano opracowanie testów i ankiet do oceny dostawców zewnętrznych.		
	(OCH.1) Zarządzanie tożsamościami, uwierzytelnianie i kontrola dostępu	W Jednostce wdrożono system zarządzania tożsamościami i uprawnieniami.	TAK	TAK			
		Fizyczny dostęp do zasobów Jednostki jest zarządzany i chroniony.	TAK	TAK			
		Funkcjonuje zarządzanie zdalnym dostępem do zasobów Jednostki.	TAK	TAK			
		Konta użytkowników i ich prawa dostępu do zasobów są przez Jednostkę zarządzane z uwzględnieniem zasady najniższych uprawnień i rozdzielenia obowiązków.	TAK	TAK			
		Integralność sieci Jednostki jest chroniona (np. przez segmentację).	TAK	TAK			
		Weryfikacja dostępu do zasobów Jednostki opiera się na wykorzystania uwierzytelniania wieloskładnikowego (MFA).	NIE	TAK	Wprowadzenie uwierzytelniania wieloskładnikowego.		
	(OCH.2) Świadomość i podnoszenie kompetencji	Użytkownicy ze wysokimi uprawnieniami rozumieją swoje role i obowiązki w Jednostce.	TAK	TAK			
		Podmioty zewnętrzne współpracujące z Jednostką (np. dostawcy, klienci, partnerzy) rozumieją swoje role i obowiązki.	TAK	TAK			
		Kadra kierownicza wyższego szczebla w Jednostce rozumie swoje role i obowiązki.	NIE	TAK	Zaplanowano szkolenie kadry kierowniczej.		
		Personel cyberbezpieczeństwa oraz bezpieczeństwa fizycznego w Jednostce rozumie swoje role i obowiązki.	TAK	TAK			
	(OCH.3) Bezpieczeństwo danych	W Jednostce dane w spoczynku są chronione.	TAK	TAK			
		W Jednostce dane przesyłane są zabezpieczone.	CZĘŚCIOWO	TAK	Zaplanowano zakup UTM.		
		Zasoby Jednostki są formalnie zarządzane podczas usuwania, przenoszenia i dysponowania.	CZĘŚCIOWO	TAK	Zaplanowano zakup oprogramowania UEM.		
		Utrzymywana jest odpowiednia zdolność Jednostki do zapewnienia dostępności do jej danych.	TAK	TAK			
		Wdrożono w Jednostce mechanizmy ochrony przed wyciekami danych.	CZĘŚCIOWO	TAK	Zaplanowano zakup oprogramowania DLP.		

Ochrona (OCH	(OCH.4) Bezpieczeństwo kopii zapasowych, plany reagowania na zagrożenia	Kopie zapasowe danych Jednostki są sporządzane, utrzymywane i testowane.	TAK	TAK	Zaplanowano zakup systemu do kopii zapasowych.		
		Dostęp do kopii zapasowych danych Jednostki jest dodatkowo chroniony.	TAK	TAK			
		Odpowiednie dane, będące w posiadaniu Jednostki, są niszczone zgodnie z funkcjonującymi politykami.	TAK	TAK			
		Opracowano plan backupu i odmiejscowienia kopii zapasowych danych Jednostki.	TAK	TAK			
		Jednostka posiada i zarządza planami reagowania: w zakresie reagowania na incydenty, w zakresie ciągłości działania oraz planami odtwarzania w zakresie odtwarzania po incydentach i awariach.	TAK	TAK			
		Plany reagowania i odtwarzania są w Jednostce weryfikowane i testowane.	TAK	TAK	W ramach wdrożenia SZBI zaplanowano aktualizację planów reagowania.		
		Opracowano i wdrożono w Jednostce plan zarządzania podatnościami.	TAK	TAK	W ramach wdrożenia SZBI zaplanowano aktualizację planów zarządzania podatnościami.		
	Technologia ochronna (OCH.5)	Zapisy zdarzeń / logów / inspekcji są określone, dokumentowane, wdrażane i sprawdzane zgodnie z politykami Jednostki.	TAK	TAK	Aktualnie logi są zbierane i analizowane, Polityki zostana zaktualizowane w ramach wdrożenie SZBI.		
		Nośniki wymienne są chronione, a ich stosowanie jest ograniczone zgodnie z politykami Jednostki.	TAK	TAK	W ramach wdrożenia SZBI zostaną uściślone procedury w SZBI.		
		Zasada najmniejszej funkcjonalności jest stosowana w Jednostce przy konfiguracji systemów tak, by posiadały one tylko niezbędne możliwości.	TAK	TAK			
		Łącza Jednostki do Internetu są chronione (np. przez AntyDDoS własny / operatorski / inne rozwiązania).	NIE	TAK	Zaplanowano zakup usługi AntyDDos.		
		Odpowiednie mechanizmy (jak np. *failsafe* , równoważenie obciążenia - *load ballancing)* są wdrażane w Jednostce w celu osiągnięcia odpowiednich wymagań, dotyczących odporności w normalnych oraz niekorzystnych warunkach.	NIE	TAK	Zaplanowano zakup UTM.		
ia i Monitoring (CM)	Anomalie i zdarzenia (CM.1)	Wykryte zdarzenia są w Jednostce analizowane w celu wykrycia metody, przebiegu oraz celu ataków.	TAK	TAK			
		Dane o zdarzeniach są pozyskiwane z wielu źródeł w infrastrukturze IT Jednostki a następnie są centralnie korelowane i analizowane.	NIE	TAK	Zaplanowano zakup oprogramowania SIEM.		
	Ciągłe monitorowanie bezpieczeństwa	Sieć Jednostki jest monitorowana w celu wykrywania potencjalnych zdarzeń cyberbezpieczeństwa.	CZĘŚCIOWO	TAK	Zaplanowano zakup oprogramowania SIEM.		
		Środowisko fizyczne Jednostki jest monitorowane w celu wykrycia potencjalnych zdarzeń cyberbezpieczeństwa.	CZĘŚCIOWO	TAK	Zaplanowano zakup oprogramowania SIEM.		
		Aktywność personelu Jednostki jest monitorowana w celu wykrycia potencjalnych zdarzeń związanych z cyberbezpieczeństwem.	TAK	TAK			
		Złośliwy kod w oprogramowaniu Jednostki jest wykrywany.	NIE	NIE			
		Nieautoryzowany kod źródłowy oprogramowania Jednostki jest wykrywany (np. ActiveX, JavaScript).	NIE	NIE			

Zdarzen	Ciągłe monitorowanie bezpieczeństwa (CM.2)	Aktywność zewnętrznych dostawców usług dla Jednostki jest monitorowana w celu wykrywania potencjalnych zagrożeń cyberbezpieczeństwa.	CZĘŚCIOWO	TAK	Zaplanowano zakup oprogramowania SIEM.		
		Prowadzi się w Jednostce ciągłe monitorowanie pod kątem nieautoryzowanego dostępu, połączeń, urządzeń i oprogramowania.	CZĘŚCIOWO	TAK	Zaplanowano zakup firewall UTM oraz oprogramowania typu NAC.		
		Przeprowadza się w Jednostce cykliczne skanowanie podatności.	NIE	TAK	W ramach SZBI zaplanowano wykonanie testów podatnościowych oraz opracowanie procedury zarządzania podatnościami.		
Reagowanie (RE)	Planowanie reagowania (RE)	Plan reagowania na incydenty w Jednostce jest realizowany w trakcie trwania incydentu lub po jego wystąpieniu.	TAK	TAK	W ramach aktualizacji SZBI zaplanowano opracowanie procedury zarządzania incydentami i naruszeniami.		
		Personel Jednostki zna swoje role i kolejność operacji, na wypadek konieczności reagowania na incydenty bezpieczeństwa.	TAK	TAK	Zaplanowano szkolenie pracowników. Procedury zostaną zaktualizowane w ramach SZBI.		
		Incydenty są zgłaszane w Jednostce zgodnie z ustalonymi procedurami.	TAK	TAK	W ramach aktualizacji SZBI zaplanowano opracowanie procedury zarządzania incydentami i naruszeniami.		
		Informacje o incydentach bezpieczeństwa są udostępniane w Jednostce zgodnie z planami reagowania na incydenty.	TAK	TAK	W ramach aktualizacji SZBI zaplanowano opracowanie procedury zarządzania incydentami i naruszeniami.		
		Koordynacja Jednostki ze stronami trzecimi jest prowadzona w sposób zgodny z planami reagowania.	TAK	TAK	W ramach aktualizacji SZBI zaplanowano opracowanie planów reagowania.		
		Dobrowolna wymiana informacji Jednostki z zewnętrznymi podmiotami jest prowadzona w celu osiągnięcia szerszej świadomości sytuacyjnej w zakresie cyberbezpieczeństwa.	CZĘŚCIOWO	TAK	W ramach aktualizacji SZBI zaplanowano opracowanie planów wymiany informacji z podmiotami trzecimi.		
		Jednostka jest podłączona do systemu S46.	NIE	NIE			
	Obsługa incydentów (OI)	Incydenty są wykrywane, zgłaszane i obsługiwane w obrębie Jednostki.	TAK	TAK			
		Są prowadzone działania naprawcze po wystąpieniu Incydentów.	TAK	TAK			
		Nowe, zidentyfikowane w Jednostce podatności są usuwane lub akceptowane i dokumentowane są ryzyka związane z nimi.	CZĘŚCIOWO	TAK	W ramach aktualizacji SZBI zaplanowano wykonanie testów podatnościowych oraz opracowanie procedury zarządzania podatnościami.		
	Doskonalenie (DS)	Plany reagowania na incydenty uwzględniają wyciąganie wniosków z wykrytych i obsłużonych incydentów.	CZĘŚCIOWO	TAK	W ramach aktualizacji SZBI zaplanowano opracowanie procedury zarządzania incydentami i naruszeniami.		
		Polityki reagowania na incydenty w Jednostce są aktualizowane.	CZĘŚCIOWO	TAK	W ramach aktualizacji SZBI zaplanowano opracowanie procedury zarządzania incydentami i naruszeniami.		

Odtwarzanie (OD)	Planowanie odtwarzania (OD.1)	Plan odtwarzania po awarii jest realizowany w Jednostce po wystąpieniu szkodliwych skutków incydentu cyberbezpieczeństwa.	TAK	TAK			
	Aktualizacja (OD.2)	W Jednostce plany odtwarzania uwzględniają zgromadzone, dotychczasowe wnioski i doświadczenia, które są wykorzystywane w procesie doskonalenia (baza doświadczeń).	CZĘŚCIOWO	TAK	Planowana aktualizacja procedur w SZBI.		
		W Jednostce polityki odtwarzania są aktualizowane.	NIE	TAK	Planowana aktualizacja procedur w SZBI.		
Infrastruktura (IN)	Sieć LAN (IN.1)	W infrastrukturze IT Jednostki są wykorzystywane przełączniki klasy *enterprise* i mają one aktualne, wykupione wsparcie.	TAK	TAK			
		W Jednostce jest stosowana segmentacja sieci.	TAK	TAK			
		W Jednostce jest stosowany mechanizm *DNS Sinkholing,* oparty na liście ostrzeżeń z CERT Polska.	NIE	NIE			
		W Jednostce jest wykorzystywane tylko oprogramowanie posiadające aktualne wsparcie.	TAK	TAK	Zaplanowano zakup firewall UTM klasy Enterprise z aktualnym wsparciem.		
	Ochrona brzegowa (IN.2)	W Jednostce jest Firewall klasy *enterprise* , ma aktualne wsparcie, jest aktualizowany na bieżąco.	TAK	TAK			
		W Jednostce jest wykorzystywany VPN a certyfikaty mają wszyscy użytkownicy VPN.	NIE	NIE			
	Poczta (IN.3)	Jednostka posiada własny serwer poczty.	NIE	NIE			
		W Jednostce są wdrożone mechanizmy SPF / DKIM / DMARC.	TAK	TAK			
		W Jednostce jest wdrożony *Sandbox* .	NIE	NIE			
		W Jednostce jest wdrożony mechanizm MFA dla wszystkich użytkowników usług pocztowych i jest aktualnie wykorzystywany.	NIE	NIE			
	WWW i usługi on-line (IN.4)	Jednostka korzysta z samorzad.gov.pl w celu utrzymania strony informacyjnej i BIP.	NIE	NIE			
		W Jednostce stosuje się zabezpieczenia transmisji TLS1.3.	NIE	TAK	Zostaną wdrożone mechanizmy zabezpieczania transmisji poprzez zakup UTM oraz rekonfiguracj stacji końcowych.		
		W Jednostce jest stosowane wymuszanie silnych haseł oraz są blokowane lub usuwane konta standardowe i testowe.	TAK	TAK			
	Wirtualizacja (IN.5)	W Jednostce jest wykorzystywana wirtualizacja serwerów.	TAK	TAK			
		Rozwiązanie wirtualizacyjne w Jednostce posiada aktualną umowę wsparcia i otrzymuje aktualizacje producenta.	NIE	TAK	Zaplanowano zakup licencji oraz wparcia producenta.		
		Jednostka korzysta z Systemu ZUCH (Usług Chmurowych).	NIE	NIE			
	Kopia zapasowa (IN.6)	Jednostka posiada odmiejscowioną kopię danych.	TAK	TAK			
		Jednostka wykorzystuje do backupów napęd lub bibliotekę taśmową.	NIE	NIE			
		Jednostka wykorzystuje system kopii zapasowych izolowany od środowiska produkcyjnego.	CZĘŚCIOWO	TAK	Zaplanowano zakup system kopii, który będzie odizolowany od środowiska produkcyjnego.		
		Jednostka posiada i wykorzystuje następujące rodzaje rozwiązań:					
		SIEM (ang. *Security Information and Event Management*)	NIE	TAK	Zaplanowano zakup oprogramowania UEM.		
		DLP (ang. *Data Loss Prevention*)	NIE	TAK	Zaplanowano zakup oprogramowania UEM.		

	Systemy bezpieczeństwa (IN.7)	NAC (ang. *Network Access Control*)	NIE	TAK	Zaplanowano zakup oprogramowania NAC.		
		WAF (ang. *Web Application Firewall*)	TAK	TAK	Zaplanowano zakup UTM.		
		PAM (ang. *Privileged Access Management*)	NIE	TAK	Zaplanowano zakup oprogramowania UEM.		
		DAM (ang. *Database Access Management*)	NIE	NIE			
		EDR (ang. *Endpoint Detection and Response*)	NIE	TAK	Zaplanowano zakup programu antywirusowego z funkcjonalnością EDR.		
		Ochrona DNS (ang. *Domain Name Server Protection*)	NIE	NIE			
		IDS / IPS (ang. *Intrusion Detection / Prevention System)*	TAK	TAK	Zaplanowano zakup UTM.		
		Antywirus / Antymalware	TAK	TAK			
		UTM (ang. *Unified Threat Management*)	TAK	TAK	Zaplanowano zakup UTM.		
		MDM (ang. *Mobile Device Management*)	NIE	TAK	Zaplanowano zakup oprogramowania MDM.		
		SOC (ang. *Security Operations Center*)	NIE	NIE			
	Narzędzia wspierające (IN.8)	SAM (ang. *Software Asset Management*)	NIE	TAK	Zaplanowano zakup oprogramowania UEM.		
		CMDB (ang. *Configuration Management DataBase*)	NIE	NIE			
		Narzędzie wspierające analizę ryzyka	NIE	NIE			
Telekomunikacja (TE)	Typ łącza telekomunikacyjnego (TE.1)	**Proszę wypełnić odpowiednimi informacjami:**					
		Typy wykorzystywanych przez Jednostkę łącz internetowych	światłowód				
		Liczba łącz internetowych wykorzystywanych przez Jednostkę	1				
		Przepustowość (w przypadku łącz niesymetrycznych: suma przepustowości: *download + upload*)	2x1000				
		Ilość aktywnych służbowych telefonów komórkowych w Jednostce	20				
		Ilość i rodzaj łącz analogowych / głosowych	7				
		Ilość głosowych łącz awaryjnych, niezależnych od lokalnego zasilania	7				
		Jednostka wykorzystuje *Firewall* dostarczony i zarządzany przez operatora.	NIE	NIE			
		Jednostka wykorzystuje system AntyDDoS (własny lub operatorski).	NIE	TAK	Zaplanowano zakup usługi AntyDDos.		
		Jednostka posiada własną, wewnętrzną centralę telefoniczną.	TAK	TAK			
		Jednostka wykorzystuje wewnętrzną telefonię VoIP.	TAK	TAK			
	Zasilanie Awaryjne (TE.2)	W Jednostce są zasilacze awaryjne (UPS) przy stanowiskach pracy.	NIE	NIE			
		Wszystkie serwery w Jednostce są wyposażone w nadmiarowe zasilacze.	TAK	TAK			
		Jednostka posiada własną serwerownię.	TAK	TAK			
		Serwerownia Jednostki posiada zasilanie awaryjne (UPS).	TAK	TAK	Zaplanowano wymianę UPS na nowy.		
		Urządzenia w serwerowni Jednostki przy braku zasilania zewnętrznego korzystają z zasilania awaryjnego (UPS).	TAK	TAK	Zaplanowano wymianę UPS na nowy.		
		Jednostka posiada własny generator awaryjny.	TAK	TAK			
		Serwerownia Jednostki jest zasilana z UPS w czasie rozruchu generatora awaryjnego.	TAK	TAK	Zaplanowano wymianę UPS na nowy.		

		Na ile godzin pracy generatora pod pełnym obciążeniem wystarczy zatankowany do pełna zbiornik paliwa do generatora?	5		

Opis wykorzystanych skrótów (w kolejności ich pojawiania się w Ankiecie, jeśli tam nie są rozwinięte)	
Kierownik JST	Organ działający w imieniu jednostki samorządu terytorialnego.
MFA (ang. *MultiFactor Authentication*)	Uwierzytelnienie wieloskładnikowe. Wykorzystywanie nie tylko haseł, ale także innych wektorów uwierzytelniania np. kodów z aplikacji, kodów z SMS, tokenów itp.
AntyDDoS (ang. *Anti-Distributed Denial of Service*)	Uwierzytelnienie wieloskładnikowe. Wykorzystywanie nie tylko haseł, ale także innych wektorów uwierzytelniania np. kodów z aplikacji, kodów z SMS, tokenów itp.
S46	Uwierzytelnienie wieloskładnikowe. Wykorzystywanie nie tylko haseł, ale także innych wektorów uwierzytelniania np. kodów z aplikacji, kodów z SMS, tokenów itp.
DNS (ang. *Domain Name Service*)	Protokół i oprogramowanie, które sprawia, że nazwa strony internetowej jest przekształcana na adres IP. DNS wyszukuje adres IP danej witryny na podstawie adresu jaki użytkownik wpisał np. w swojej przeglądarce.
DNS *Sinkholing*	Mechanizm dający ochronę użytkownikom dzięki przechwytywaniu żądań DNS, które próbują łączyć ze znanymi, złośliwymi lub niechcianymi domenami i zwraca w ich miejsce kontrolowany adres IP, który wskazuje lokalny serwer typu *sinkhole* , zdefiniowany przez administratora DNS.
CERT (ang. *Computer Emergency Response Team*)	Zespół reagowania na zagrożenia komputerowe, przypadki zagrożeń i naruszeń bezpieczeństwa teleinformatycznego.
VPN (ang. *Virtual Private Network*)	Wirtualna sieć prywatna lub rozwiązanie, które umożliwia zdalne, bezpieczne (szyfrowane) połączenie z siecią komputerową organizacji i jej zasobami przez niechronione i niezaufane sieci publiczne.
SPF (ang. *Sender Policy Framework*)	Typ rekordu domeny, działający w ramach usługi DNS, który jest odpowiedzialny za poprawną identyfikację serwera pocztowego, uprawnionego do wysyłania poczty elektronicznej w imieniu danej domeny. Ma na celu wprowadzenie zabezpieczenia serwerów pocztowych przed przyjmowaniem poczty z niedozwolonych źródeł. SPF dotyczy tylko komunikacji pomiędzy serwerami SMTP. Do działania SPF jest potrzebne ustanowienie poprawnej konfiguracji w strefie domeny. SPF pozytywnie wpływa na ograniczenie liczby wiadomości mailowych, identyfikowanych jako spam.
DKIM (ang. *Domain Keys Identified Mail*)	Służy do uwierzytelniania wysyłanych wiadomości. Działa podobnie jak rekord SPF i jest otwartym standardem uwierzytelniania poczty. Funkcjonuje w ustawieniach DNS ale jego budowa jest bardziej złożona niż SPF. Stanowi podstawę do zabezpieczania wiadomości e-mail. DKIM powoduje, że osoba, która otrzymuje wiadomość ma pewność, że nadawcą wiadomości jest faktyczny właściciel adresu a nie ktoś, kto się pod niego podszywa.
DMARC (ang. *Domain-based Authentication Reporting and Conformance*)	Protokół uwierzytelniania i raportowania poczty e-mail. Wskazuje, co ma się stać z wiadomościami zidentyfikowanymi jako sfałszowane. Mogą one np. trafić do folderu SPAM lub zostać całkowicie odrzucone. Dodatkowo DMARC umożliwia wysyłanie raportu o wiadomościach, które przeszły (pomyślnie lub negatywnie) ocenę protokołu.
BIP	Biuletyn Informacji Publicznej
TLS (ang. *Transport Layer Security*)	Protokół kryptograficzny zapewniający bezpieczne połączenie i przesyłanie danych między serwerem a klientem w sieciach komputerowych.
System ZUCH	System Zapewnienia Usług Chmurowych (https://chmura.gov.pl/zuch)
SIEM (ang. *Security Information and Event Management*)	Rozwiązanie służące do wykrywania, korelacji oraz analizy zdarzeń bezpieczeństwa, występujących w systemach i sieciach teleinformatycznych.
DLP (ang. *Data Loss Prevention*)	Rozwiązanie służące do zabezpieczania przed wyciekami informacji z organizacji.

NAC (ang. *Network Access Control*)	Rozwiązanie zapewniające kontrolę dostępu do sieci przez weryfikację bezpieczeństwa i uprawnień urządzenia końcowego, ubiegającego się o dostęp do sieci, uwierzytelnienie stacji lub użytkownika, warunkowe przydzielenie dostępu do określonej sieci.
WAF (ang. *Web Application Firewall*)	Programowe rozwiązanie bezpieczeństwa, pełniące funkcję firewalla aplikacyjnego, dedykowane do ochrony aplikacji internetowych przed atakami, lukami w zabezpieczeniach aplikacji i złośliwymi działaniami. Funkcjonuje jako filtr między aplikacją a siecią, monitorując i analizując przychodzący i wychodzący ruch w celu identyfikacji i blokowania potencjalnych zagrożeń.
PAM (ang. *Privileged Access Management*)	Rozwiązanie, które koncentruje się na scentralizowaniu zarządzania poświadczeniami wszelkich kont z wysokimi uprawnieniami do różnych systemów w infrastrukturze organizacji. PAM zarządza bezpiecznym przechowywaniem poświadczeń, ich zmianami, rotacją i dostępem uprawnionych użytkowników, co bardzo upraszcza zarządzanie dostępem do kluczowych zasobów oraz istotnie podnosi ich bezpieczeństwo.
DAM (ang. *Database Access Management*)	Rozwiązanie bezpieczeństwa pozwalające na zarządzanie dostępami do baz danych. Określa ono: jakie konta mogą mieć dostęp, do jakich obszarów baz i ich elementów oraz jakie te konta mają prawa dostępu do zawartości baz danych. Zapewnia także monitorowanie i rozliczalność takich dostępów.
EDR (ang. *Endpoint Detection and Response*)	Zintegrowane rozwiązanie bezpieczeństwa, którego główne funkcje to: monitorowanie i gromadzenie danych o aktywnościach użytkowników i oprogramowania na urządzeniach końcowych, analiza tych danych w celu identyfikacji wzorców zagrożeń, automatyczne reagowanie na zidentyfikowane zagrożenia w celu ich usunięcia lub powstrzymania, powiadamianie personelu bezpieczeństwa o zidentyfikowanych anomaliach.
Ochrona DNS (ang. *Domain Name Server Protection*)	Warstwa zabezpieczeń DNS, filtracji niechcianego ruchu. Dodaje podejrzane odnośniki URL do czarnej listy. Ochrona przed zagrożeniami i złośliwymi atakami zarówno dla komputerów lokalnych, jak i działających zdalnie - poza siedzibą organizacji.
IDS (ang. *Intrusion Detection System)*	Rozwiązanie służące do wykrywania niepożądanych aktywności w infrastrukturze organizacji oraz informowania o ich wystąpieniu odpowiednich funkcji lub osób. Bardziej zaawansowaną formą IDS są rozwiązania IPS.
IPS (ang. *Intrusion Prevention System)*	Rozwiązanie służące do zapobiegania wystąpieniom oraz skutkom niepożądanych aktywności w infrastrukturze organizacji, takich jak np. próby włamań, przełamania zabezpieczeń. Zadaniem IPS jest także wykrywanie takich działań w sieci organizacji, podejmowanie prób zapobiegania ich skutkom i informowanie o ich wystąpieniu odpowiednich funkcji lub osób.
Antywirus	Oprogramowanie, którego celem jest skanowanie, wykrywanie, rozpoznawanie oraz usuwanie złośliwego oprogramowania z komputera lub innego urządzenia, na którym zostało zainstalowane.
Antymalware	Narzędzia wykrywające zagrożenia na urządzeniach końcowych. Ich zadaniem jest: skanowanie plików, dogłębna analiza ich struktury, danych i logiki w poszukiwaniu nietypowych instrukcji i szkodliwych fragmentów kodu.
UTM (ang. *Unified Threat Management*)	Urządzenia sieciowe, odpowiadające za kompleksową ochronę, nadzorowanie ruchu w sieci lokalnej oraz styk / dostęp do Internetu. Zamiast wielu rozwiązań typu: zapory sieciowe, IPS, filtry antyspamowe, routery itp. - jedno rozwiązanie, łączące wszystkie te funkcje.
MDM (ang. *Mobile Device Management*)	Oprogramowanie, które umożliwia administratorom IT monitorowanie, zarządzanie i zabezpieczanie służbowych urządzeń mobilnych, takich jak smartfon czy tablet. MDM pozwala zespołom IT na zdalną aktualizację i zabezpieczanie urz. mobilnych za pośrednictwem centralnej konsoli zarządzania. W zakres tego może wchodzić: zarządzanie aplikacjami, wymuszanie zmian haseł, wymuszanie aktualizacji urządzeń, definiowanie polityk ściśle określających zakres działań użytkowników na urządzeniach mobilnych - w celu zapewnienia im systemowych mechanizmów bezpieczeństwa.

SOC (ang. *Security Operations Center*)	Jednostka odpowiedzialna za bieżące monitorowanie i analizę stanu cyberbezpieczeństwa organizacji. Celem SOC jest wykrywanie, analizowanie i reagowanie na incydenty związane z cyberbezpieczeństwem z wykorzystaniem trzech rodzajów zasobów: 1. ludzi i ich kompetencji, 2. wypracowanych procesów i procedur, 3. narzędzi - rozwiązań technicznych.
SAM (ang. *Software Asset Management*)	Rozwiązanie pozwalające efektywnie zarządzać oprogramowaniem wykorzystywanym w instytucji. Skupia się przede wszystkim na aspekcie licencyjnym. Umożliwia również kompleksowy wgląd w infrastrukturę IT, oprogramowanie w niej wykorzystywane oraz zagrożenia związane z jego użytkowaniem. Docelowo SAM pozwala instytucji na monitorowanie zgodności licencyjnej, optymalizowanie kosztów związanych z oprogramowaniem, eliminowanie niewspieranego oprogramowania oraz dostosowywanie inwestycji IT do potrzeb działalności.
CMDB (ang. *Configuration Management DataBase*)	Narzędzia pozwalające na utrzymywanie w organizacji bazy danych, zawierającej dwa typy aktualizowanych na bieżąco informacji: szczegóły każdego komponentu infrastruktury IT (jego konfiguracji (ang. Configuration Item, CI) oraz bazę relacji między elementami CI. Baza CI mówi o sprzęcie i komponentach oprogramowania wykorzystywanych w usługach IT, którymi można zarządzać a także o samych usługach. CMDB pozwala na wykrywanie i odnotowywanie zmian inwentaryzacyjnych a dzięki bazie relacji można oszacować wpływ tych zmian na wszystkie procesy, usługi i infrastrukturę. CMDB może także wspomagać automatyczną inwentaryzację zasobów IT organizacji oraz wspierać zarządzanie procesem zmian. CMDB pozwala także na zbieranie, przechowywanie i zarządzanie konfiguracją usług, systemów i urządzeń. Ciągłe monitorowanie aktywnych konfiguracji pozwala wykryć nieautoryzowane lub nieudane zmiany konfiguracji, co ma istotny wpływ na cyberbezpieczeństwo.
VoIP (ang. *Voice over IP*)	Technologia przesyłania sygnału akustycznego, zamienionego na postać cyfrową, za pomocą pakietów IP. Umożliwia m.in. wykonywanie połączeń telefonicznych w sieci lokalnej i przez Internet. VoIP pozwala na oszczędności na rozmowach telefonicznych i na korzystanie z wielu innych funkcji, takich jak wideokonferencje czy komunikatory internetowe.
UPS *(ang. Uninterruptable Power Supply)*	Zapasowe zasilanie bateryjne