Zarządzenie nr 69/2021
Wójta Gminy Lądek
z dnia 28 października 2021 roku.

w sprawie uzupełnienia dokumentacji „Systemu Zarządzania Bezpieczeństwem Informacji" w Urzędzie Gminy Lądek

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2021 r. poz. 1372 ze zm.), art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) oraz § 20 ust. 1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r. poz. 2247 ze zm.) zarządza się, co następuje:

§ 1. Wprowadza się do stosowania w Urzędzie Gminy Lądek uzupełnienie dokumentacji „Systemu Zarządzania Bezpieczeństwem Informacji" w postaci:

1) Procedur awaryjnego odtwarzania systemów, która stanowi załącznik nr 1 do niniejszego zarządzenia.

2) Procedur wdrażania, likwidacji oraz inwentaryzacji sprzętu i oprogramowania, która stanowi załącznik nr 2 do niniejszego zarządzenia.

3) Procedur pracy na odległość oraz pracy zdalnej, która stanowi załącznik nr 3 do niniejszego zarządzenia.

4) Procedur reagowania na incydenty, która stanowi załącznik nr 4 do niniejszego zarządzenia.

§ 2. Zobowiązuje się Sekretarza Gminy do zapoznania podległych pracowników z postanowieniami zarządzenia i prowadzenia nadzoru nad przestrzeganiem ich realizacji.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Artur Miętkiewicz

Procedura awaryjnego odtwarzania systemów		
Wersja: 1.0	Data wprowadzenia:	28.10.2021

Załącznik nr 1
do Zarządzenia nr 69/2021
Wójta Gminy Lądek
z dnia 28 października 2021r

Procedura awaryjnego odtwarzania systemów

Spis treści

1. Wstęp

Procedura awaryjnego odtwarzania stanowi wskazówki dla personelu dotyczące procedury postępowania w przypadku poważnej awarii systemu, aplikacji lub awarii fizycznej sprzętu. W uzasadnionych przypadkach możliwe są odstępstwa od procedury. Odstępstwa mogą być powiązane z charakterem awarii lub koniecznością wykonywania niestandardowych działań mających na celu jak najszybsze przywrócenie systemów do normalnego funkcjonowania.

2. Elementy niezbędne w procedurze awaryjnego odtwarzania.

Elementami niezbędnymi do przywrócenia systemów do normalnego funkcjonowania są:

- Zasoby komputerowe,
- Infrastruktura teleinformatyczna (sieciowa),
- Serwery,
- Nośniki instalacyjne systemów operacyjnych,
- Nośniki instalacyjne aplikacji,
- Kopie baz danych,
- Kopie innych danych,
- Kopie konfiguracji urządzeń sieciowych.

W zależności od charakteru oraz zakresu awarii wykorzystane powinny zostać adekwatne zasoby. W przypadku braku któregokolwiek z niezbędnych zasobów powinna zostać uruchomiona procedura zakupów w trybie awaryjnym. Dopuszczalne jest stosowanie sprzętu tymczasowego (o innych parametrach niż docelowy), jeśli jest to uzasadnione czasem oczekiwania na nowy sprzęt lub pilnością przywrócenia systemów do normalnego funkcjonowania.

Wszelkie nośniki instalacyjne przechowywane są w pomieszczeniach o ograniczonym dostępie w zamkniętych szafach. Kopie zapasowe systemów zwirtualizowanych znajdują się na przeznaczonej do tego celu macierzy dyskowej. Kopie baz danych znajdują się na wyznaczonej macierzy dyskowej oraz dodatkowo są również zlokalizowane na dysku komputera w szafie dystrybucyjnej. Pełni on rolę zapasowego magazynu kopii zapasowej. Działania niezbędne do wykonania w procesie awaryjnego odtwarzania.

Czynności wykonywane podczas awaryjnego odtwarzania uzależnione są od charakteru oraz zasięgu awarii. Przed przystąpieniem do procedury odtwarzania ASI ocenia rodzaj, skalę oraz wpływ awarii na funkcjonowanie systemów. Podczas wykonywania procedury awaryjnego odtwarzania ASI powinien posiłkować się instrukcjami

instalacyjnymi dostarczonymi przez producenta, w których znajdują się niezbędne skrypty oraz zrzuty ekranowe. W ramach postępowania w sytuacjach awaryjnych wyszczególniono trzy główne sytuacje, od których uzależniony jest sposób postępowania ASI:

- Awaria oprogramowania

  Awaria oprogramowania może dotyczyć jednej bądź kilku aplikacji lub systemów operacyjnych. W każdym przypadku awarii należy powiadomić użytkowników o przerwie w dostępie do usługi oraz określić przybliżony czas jej niedostępności. W przypadku wystąpienia tego typu awarii ASI ocenia zasięg awarii oraz krytyczność odzyskania każdej z aplikacji lub systemów. Następnie rozpoczyna odtwarzanie aplikacji poprzez ich ponowną instalację z oryginalnych nośników lub wykonanych obrazów systemu. Po zainstalowaniu aplikacji należy sprawdzić poprawność jej funkcjonowania oraz określić, czy konieczne jest odtworzenie baz danych. W przypadku konieczności odtworzenia baz danych należy w tym celu użyć ostatniej poprawnej kopii. Po przywróceniu systemu do pełni sprawności ASI powinien ocenić poprawność funkcjonowania aplikacji oraz powiadomić użytkowników o przywróceniu dostępności usługi. Informacje na temat awarii powinny znaleźć się wraz z opisem w dzienniku incydentów.

- Awaria wirtualnej maszyny

  W przypadku wystąpienia awarii wirtualnej maszyny ASI określa skalę awarii. O awarii powinni zostać powiadomieni użytkownicy korzystający z zasobów wirtualnej maszyny. Informacja przekazana użytkownikom powinna zawierać dane na temat szacowanego czasu niedostępności usług. Podczas oceny skali awarii ASI powinien zadecydować jaki sposób postępowania jest najbardziej efektywny dla odzyskania pełni sprawności przez system. W przypadku, gdy zachodzi konieczność odtworzenia całej wirtualnej maszyny operacja ta dokonywana jest z ostatniej prawidłowo wykonanej kopii zapasowej. Po przywróceni systemu do pełni działania ASI powinien sprawdzić poprawność jej funkcjonowania oraz powiadomić użytkowników o przywróceniu dostępności usługi. Informacje na temat awarii powinny znaleźć się wraz z opisem w dzienniku incydentów.

- Awaria fizycznego serwera

  W przypadku awarii fizycznej serwera jego funkcja jest przejmowana przez jeden z serwerów zapasowych. ASI zobowiązany jest do potwierdzenia awarii serwera oraz powiadomienia odpowiedniego serwisu o awarii i nadzorowaniu naprawy. Informacje na temat awarii powinny znaleźć się wraz z opisem w dzienniku incydentów.

3. Kolejność odtwarzania infrastruktury.

Infrastruktura teleinformatyczna jest jednym z czynników kluczowych dla sprawnego funkcjonowania Urzędu. W przypadku awarii należy postępować zgodnie z poniższym algorytmem.

1. Diagnoza sytuacji – personel odpowiedzialny za proces przywrócenia sytuacji powinien dokładnie zidentyfikować punkty awarii oraz określić, które urządzenia wymagają naprawy lub wymiany, a w przypadku których konieczna jest tylko ponowna konfiguracja.
2. Odtworzenie krytycznej infrastruktury sieciowej. Odtworzenie krytycznej infrastruktury sieciowej oraz przywrócenie łączności jest elementem krytycznym ze względu na możliwe przyśpieszenie odtwarzanie pozostałej infrastruktury.
3. Odtwarzanie infrastruktury serwerowej. Odtworzenie fizycznej infrastruktury serwerowej daje podstawy do wykonania kolejnych kroków odzyskiwania sprawności działania infrastruktury.
4. Odtwarzanie infrastruktury wirtualnej. Kolejnym krokiem odzyskiwania sprawności działania jest odtworzenie infrastruktury wirtualnej. Dopuszcza się odtworzenie infrastruktury wirtualnej z kopii lub obrazów systemów.
5. Odtworzenie infrastruktury programowej. Po odtworzeniu zwirtualizowanych systemów należy odtworzyć infrastrukturę programową poszczególnych systemów. Krok ten może być połączony z krokiem poprzednim.
6. Odtworzenie baz danych. W przypadku konieczności odtworzenia baz danych powinno się skorzystać z ostatniej poprawnej kopii zapasowej.
7. Odtworzenie infrastruktury użytkowników. Ostatnim krokiem przywracania systemów do pełnej funkcjonalności jest odtworzenie infrastruktury używanej przez użytkowników systemów (komputerów używanych przez użytkowników).

W przypadku odtwarzania infrastruktury, które zostało spowodowane nieautoryzowanym wtargnięciem do sieci lub systemów infrastruktura powinna zostać odtworzona z oryginalnych nośników, a następnie zainstalować wszelkie poprawki zwiększające bezpieczeństwo.

W trakcie odtwarzania infrastruktury należy zwrócić szczególną uwagę na komunikaty oraz sygnały zarówno dźwiękowe jak i wizualne przekazywane przez elementy infrastruktury. Wszelkie sygnały należy interpretować zgodnie z zaleceniami producentów i postępować zgodnie z ich instrukcjami obsługi.

Proces odtwarzania infrastruktury powinien być prowadzony w kolejności od systemów najbardziej krytycznych do tych najmniej krytycznych.

Personel odtwarzający infrastrukturę powinien sporządzić raport z przeprowadzonej akcji odtwarzania infrastruktury wraz ze wskazaniem napotkanych problemów. Raport powinien zostać poddany analizie w celu określenia możliwości wprowadzenia usprawnień w procedurze awaryjnego odtwarzania oraz wprowadzenia ewentualnych środków zabezpieczających infrastrukturę przed analogicznymi przyczynami stwarzającymi konieczność odtwarzania infrastruktury.

4. Sposób testowania posiadanych kopii zapasowych.

Kopie zapasowe powinny być regularnie testowane zgodnie z częstotliwością wskazaną w planie tworzenia kopii zapasowych. W każdym przypadku testowania kopii zapasowych, środowisko w jakim są odtwarzane powinno

uwzględniać potrzeby oraz możliwości w tym zakresie. Tam, gdzie to możliwe zaleca się stosowanie rozwiązań wirtualnych.

5. Raport końcowy.

Każdorazowo po dokonania odtworzenia infrastruktury lub przeprowadzeniu testowego odtwarzania po awarii należy sporządzić raport zawierający informację o napotkanych błędach i przybliżonym czasie odtwarzania. Raporty stanowią informacje wykorzystywane w analizie ryzyka oraz powinny stanowić jeden z tematów prowadzonego przeglądu zarządzania. Raporty należy przechowywać wraz z dokumentacją systemu. Testowanie odtwarzania awaryjnego musi odbywać się minimum raz na rok.

Załącznik nr 2
do Zarządzenia nr 69/2021
Wójta Gminy Lądek
z dnia 28 października 2021r

Procedura wdrażania, likwidacji oraz inwentaryzacji sprzętu i oprogramowania

1. Procedura wdrażania oraz likwidacji sprzętu komputerowego.

1.1. Środki do przetwarzania informacji wykorzystywane w Urzędzie są przeznaczone wyłącznie do wykonywania zadań służbowych. Zabrania się podłączania do sieci teleinformatycznej jakichkolwiek urządzeń nie posiadających autoryzacji.

1.2. Procedurę zakupu sprzętu do przetwarzania informacji realizuje ASI, zgodnie z obowiązującymi przepisami i procedurami. Obowiązuje wyłącznie pisemna forma wszelkich poleceń dotyczących zakupu sprzętu komputerowego.

1.3. ASI przygotowuje specyfikację techniczną sprzętu oraz opiniuje zasadność zakupu sprzętu zgłoszonego przez pracownika.

1.4. Przed instalacją sprzętu komputerowego na stanowisku pracy ASI sprawdza działanie urządzeń, aby w razie problemów zgłosić reklamacje.

1.5. Po zainstalowaniu sprzętu komputerowego na stanowisku pracy ASI dokonuje instruktarzu pracownika i zapoznaniu z ewentualnymi nowymi funkcjami urządzeń i programów zainstalowanych na komputerze.

1.6. Jeśli sprzęt komputerowy jest uszkodzony i jego naprawa jest nieopłacalna lub niemożliwa, lub jest przestarzały i niespełna wymagań technicznych zainstalowanego oprogramowania w Urzędzie, zostaje poddany procedurze likwidacji.

1.7. Sprzęt komputerowy do likwidacji typuje ASI.

1.8. Komisja likwidacyjna składająca się co najmniej z trzech członków dokonuje likwidacji sprzętu komputerowego.

1.9. Komisja sporządza Protokół likwidacji sprzętu komputerowego.

1.10. Po zgromadzeniu odpowiedniej ilości zlikwidowanego sprzętu komputerowego zostaje on poddany procedurze utylizacji.

1.11. ASI przekazuje firmie utylizacyjnej zlikwidowany sprzęt komputerowy, następnie sporządzony zostaje protokół przekazania sprzętu komputerowego do utylizacji.

1.12. Firma utylizacyjna jest zobowiązana do przekazania Urzędowi protokołu utylizacji sprzętu komputerowego.

2. Procedury korzystania z oprogramowania

2.1. W celu zabezpieczenia danych i programów służących do przetwarzania danych osobowych zastosowanie ma procedura korzystania z oprogramowania.

2.2. Urząd korzysta z oprogramowania komputerowego różnych producentów wyłącznie na podstawie posiadanych licencji. Urząd nie jest właścicielem tego oprogramowania, a jedynie uzyskał prawo do korzystania z niego wyłącznie na warunkach zawartych w umowach licencyjnych. Urząd nie ma prawa

powielania oprogramowania, bez wyraźnej zgody producenta oprogramowania zawartej w licencji lub osobnym piśmie.

2.3. Pracownicy mogą korzystać jedynie z oprogramowania, na które Urząd posiada aktualne licencje. Pracownik jest odpowiedzialny za stan oprogramowania zainstalowanego na komputerze.

2.4. W przypadku komputerów wolnostojących, do których nie jest przypisany na stałe konkretny użytkownik, wyznacza się osobę odpowiedzialną za ten komputer. Osobą odpowiedzialną może być w szczególności kierownik komórki organizacyjnej, która wykorzystuje taki komputer.

2.5. Wszyscy pracownicy przyjmują do wiadomości informację o konieczności pracy wyłącznie na oprogramowaniu wymienionym w „metryce komputera".

2.6. Każda zmiana stanu zainstalowanego na danym komputerze oprogramowania musi znaleźć potwierdzenie w metryce tego komputera.

2.7. Pracownicy Urzędu nie mogą za pomocą komputerów firmowych pobierać z Internetu lub przesyłać nielicencjonowanego oprogramowania oraz innych utworów w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2000 r., Nr 80, poz. 904, z późn. zm.) chronionych prawem autorskim (w tym w szczególności utworów muzycznych, filmów, grafiki, gier komputerowych i tym podobnych).

2.8. Pracownicy nie mogą wnosić na teren Urzędu ani instalować na firmowych komputerach prywatnych kopii oprogramowania, plików muzycznych i video, z żadnego nośnika i z żadnego innego urządzenia.

2.9. Pracownicy Urzędu mogą korzystać z komputerów, Internetu oraz poczty elektronicznej wyłącznie w celu wykonywania obowiązków służbowych oraz dla samokształcenia, w tym szczególnie dla podnoszenia swoich kwalifikacji na zajmowanym stanowisku.

2.10. Instalacji oprogramowania w Urzędzie może dokonywać wyłącznie ASI lub osoby do tego upoważnione.

2.11. Zakupu oprogramowania w Urzędzie mogą dokonywać wyłącznie osoby do tego upoważnione.

2.12. Osoby biorące udział w nielegalnym kopiowaniu oprogramowania mogą zostać zgodnie z prawem polskim pociągnięte do odpowiedzialności karnej i cywilnej, w tym do odpowiedzialności odszkodowawczej z tytułu odpowiedzialności cywilnej, oraz ukarane grzywną i/lub karą pozbawienia wolności w ramach odpowiedzialności karnej. Wobec takich osób zostaną również zastosowane sankcje przewidziane w Kodeksie Pracy.

3. Procedury nabywania oprogramowania

3.1. W Urzędzie obowiązuje centralizacja zakupów oprogramowania.

3.2. W Urzędzie obowiązuje wyłącznie pisemna forma wszelkich poleceń dotyczących zakupu oprogramowania.

3.3. Decyzję o zakupie nowego oprogramowania w Urzędzie podejmuje wyłącznie Kierownik Urzędu, po konsultacji z ASI.

3.4. W przypadku konieczności nabycia specyficznego oprogramowania niezbędnego dla wykonywania obowiązków przez pracownika, pracownik wnioskuje o dokonanie zakupu u swojego bezpośredniego przełożonego.

3.5. Pracownicy nie mogą samodzielnie dokonywać zakupu oprogramowania.

3.6. Urząd dokonuje zakupów wyłącznie u wiarygodnych dostawców.

3.7. Za poprawność i zgodność dokumentacji licencyjnej zakupionego oprogramowania z wymaganą dokumentacją licencyjną odpowiedzialny jest ASI.

4. Procedury przechowywania dokumentacji licencyjnej

4.1. W Urzędzie przechowuje się kompletną dokumentację licencyjną - wszystkie atrybuty legalności oprogramowania, które towarzyszyły mu przy zakupie.

4.2. Oryginalna dokumentacja licencyjna oraz podpisane metryki komputera przechowywane są w zamkniętym pomieszczeniu, do którego dostęp mają wyłącznie osoby upoważnione.

4.3. Za certyfikaty autentyczności systemów operacyjnych naklejone na obudowie komputerów odpowiedzialny jest ASI oraz osoby odpowiedzialne za dany komputer. O wszelkich przypadkach braku lub uszkodzenia certyfikatu należy niezwłocznie poinformować ASI.

4.4. Za dokumentację licencyjną oraz za jej właściwe przechowywanie odpowiedzialny jest ASI oraz osoby przez niego upoważnione.

4.5. Dokumentacja licencyjna traktowana jest jak majątek Urzędu.

4.6. Przyjęcie na stan dokumentacji licencyjnej przez ASI potwierdzane jest wpisem do książki ewidencji majątku.

4.7. Dostęp do oryginalnej dokumentacji licencyjnej ma wyłącznie ASI zarządzający oprogramowaniem oraz osoby przez niego upoważnione.

4.8. Nośniki z materiałami szkoleniowymi dla Urzędu, nośniki zakupione wraz z gazetami i czasopismami oraz nośniki zawierające oprogramowanie pochodzące z innych legalnych źródeł przechowywane są w pomieszczeniu razem z całą dokumentacją licencyjną i mogą być używane i użyczane osobom trzecim wyłącznie przez ASI oraz osoby przez niego upoważnione.

4.9. Nośniki zawierające materiały przygotowane przez Urząd powinny być oznaczone, jako własność Urzędu.

5. Procedury prowadzenia i aktualizacji rejestru sprzętu, oprogramowania i licencji.

5.1. W Urzędzie informacje o zasobach sprzętowych (stacje robocze, serwery i komputery przenośne), posiadanym i zainstalowanym oprogramowaniu oraz ilości posiadanych licencji, przechowywane są w rejestrze sprzętu, oprogramowania i licencji.

5.2. Rejestr prowadzony jest w postaci kartoteki zawierającej metryki sprzętu i oprogramowania, rolę pomocniczą pełnić może dokumentacja w postaci elektronicznej. Rejestr może być również prowadzony za pomocą dedykowanego oprogramowania.

5.3. Aktualizacja rejestru dokonywana jest na bieżąco przez ASI.

6. Procedury instalacji oprogramowania

6.1. Osobą odpowiedzialną za instalację oprogramowania w Urzędzie jest ASI zarządzający oprogramowaniem.

6.2. Instalacji może dokonywać wyłącznie ASI oraz osoby przez niego upoważnione.

6.3. Przed zainstalowaniem oprogramowania osoba odpowiedzialna za instalację musi zapoznać się z warunkami licencji i podjąć decyzję czy je akceptuje oraz czy Urząd spełnia wymogi tej licencji.

6.4. Instalacji należy dokonywać wyłącznie zgodnie z ilością posiadanych przez Urząd licencji.

6.5. Pobieranie i instalowanie oprogramowania z Internetu dopuszcza się w Urzędzie wyłącznie w sytuacji, gdy licencja na to zezwala, a oprogramowanie jest niezbędne do wykonywania obowiązków służbowych przez pracownika. Mogą tego dokonywać wyłącznie osoby upoważnione.

6.6. W odniesieniu do aplikacji klient/serwer oraz aplikacji sieciowych, pracownicy Urzędu mogą używać oprogramowania wyłącznie na warunkach określonych w stosownej umowie licencyjnej na to oprogramowanie.

6.7. Oprogramowanie w wersjach testowych lub jakikolwiek inny sposób ograniczone umowami licencyjnymi może być użytkowane w Urzędzie wyłącznie zgodnie z jego przeznaczeniem, tylko przez czas i w zakresie określonym w licencji oraz jedynie przez osoby upoważnione.

6.8. Każdorazowa instalacja oprogramowania na komputerze musi mieć odzwierciedlenie w metryce konkretnego komputera oraz w rejestrze sprzętu i oprogramowania.

6.9. ASI po każdej instalacji nowego oprogramowania zobowiązany jest do uaktualnienia rejestru, stworzenia aktualnej metryki.

6.10. Nie wolno dokonywać kopii oryginalnych nośników, jeśli umowa licencyjna na to nie zezwala. Jeżeli umowa licencyjna na to pozwala kopii takich może dokonywać wyłącznie ASI.

Załącznik nr 3
do Zarządzenia nr 69/2021
Wójta Gminy Lądek
z dnia 28 października 2021r

Procedura pracy na odległość oraz pracy zdalnej

1.1 Praca na odległość

Telefony służbowe powinny być zabezpieczone kodem PIN lub za pomocą szyfrowania. Nie można udostępniać urządzeń służbowych osobom niepowołanym np. dzieciom.

W celu ochrony dostępu do sieci wewnętrznej Organizacji, zdalny dostęp do niej może nastąpić wyłącznie z bezpiecznego urządzenia, zawierającego ostatnią aktualizacje systemu oraz łatek bezpieczeństwa, oraz posiadającego aktywne oprogramowanie antywirusowe.

Połączenie z sieci publicznych do wewnętrznych systemów teleinformatycznych powinno odbywać się przez bezpieczne protokoły szyfrujące ruch (VPN) , uniemożliwiając tym samym przejęcie sesji przez osoby niepowołane.

Wykorzystując systemy zdalnego pulpitu należy skonfigurować system tak, aby przy bezczynności automatycznie wylogował się z danej sesji.

1.2 Zasady pracy zdalnej:

1. Decyzję o skierowaniu pracownika do wykonywania pracy zdalnej podejmuje Kierownik Jednostki.
2. Pracę należy wykonywać wyłącznie na przekazanym sprzęcie służbowym.
3. Należy zachować szczególną ostrożność przy transporcie sprzętu służbowego.
4. Nie należy wyłączać ustawionej automatycznej blokady ekranu.
5. Przed opuszczeniem stanowiska pracy należy zablokować system przed nieautoryzowanym dostępem (przydatny skrót klawiszy Win+L umożliwi szybkie zablokowanie systemu).
6. Należy korzystać z Internetu służbowego (np. hotspot Wifi z telefonu służbowego, zabezpieczony hasłem), a jeżeli nie jest to możliwe można korzystać z domowej sieci bezprzewodowej, zabezpieczonej hasłem o długości min. 8 znaków (duża, mała litera, cyfra i znak specjalny).
7. Przed zalogowaniem się do systemów informatycznych należy połączyć się z VPN.
8. Należy wykonywać pracę w wybranej części lokalu mieszkalnego o ograniczonym, w miarę możliwości na czas wykonywania pracy, dostępie do niej osób postronnych (członkowie rodziny, znajomi itp.).
9. Zabronione jest udostępnianie powierzonego sprzętu komputerowego oraz loginu i hasła do urządzenia, na którym wykonywana jest praca, domownikom lub innym osobom postronnym.
10. Zabronione jest wykorzystywanie powierzonego sprzętu komputerowego do celów innych niż służbowe.
11. Należy kontrolować użycie urządzeń zewnętrznych, takich jak pamięć USB i innych, które mogą zainfekować sprzęt bądź sieć.
12. Zabronione jest przesyłanie jakichkolwiek informacji oraz danych na prywatne adresy mailowe lub ich zapisywanie na prywatnych nośnikach typu pendrive.
13. Nie należy drukować dokumentów – należy je przechowywać w wersji elektronicznej w systemach, po połączeniu się z siecią przez VPN lub na powierzonym sprzęcie służbowym,

a w przypadku konieczności ich wydrukowania i wysłania korespondencji – należy je przekazać do siedziby Urzędu.

14. Po zakończeniu ww. okresu pracy zdalnej powierzony sprzęt służbowy należy zwrócić.
15. Jeżeli urządzenie oraz dokumenty, w trakcie pracy zdalnej, ulegną zniszczeniu lub zostaną zgubione, bezzwłocznie należy poinformować o tym przełożonego.
16. Przy pracy zdalnej należy kierować się zasadą „co nie jest dozwolone, jest zabronione".
17. Przed dopuszczeniem do pracy zdalnej pracownik jest zobowiązany złożyć pisemne oświadczenie o zobowiązaniu do przestrzegania zasad ustalonych dla pracy zdalnej.
18. Dopuszcza się zmianę lub uszczegółowienie powyższych zasad w zależności od trybu oraz okoliczności wymagających świadczenia pracy zdalnej.
19. Każdorazowo decyzja co do powyższych ustaleń należy do Kierownika Jednostki, po konsultacji z ASI w zakresie bezpieczeństwa teleinformatycznego oraz IOD w zakresie bezpieczeństwa przetwarzania danych osobowych.

Procedura reagowania na incydenty		
Wersja: 1.0	Data wprowadzenia:	28.10.2021

Załącznik nr 4
do Zarządzenia nr 69/2021
Wójta Gminy Lądek
z dnia 28 października 2021r

Procedura reagowania na incydenty

Procedura reagowania na incydenty		
Wersja: 1.0	Data wprowadzenia:	28.10.2021

Spis treści

Procedura reagowania na incydenty		
Wersja: 1.0	Data wprowadzenia:	28.10.2021

1 Definicje

Naruszenie bezpieczeństwa - wszelkie działania niezgodne z dokumentami opisującymi bezpieczeństwo oraz celowe próby ingerencji w sprzęt i oprogramowanie bez zgody odpowiednich pracowników.

Incydent informatyczny – Każde nieautoryzowane lub niezaakceptowane działanie, które zostało dokonane przy użyciu komputera i/lub sieci komputerowej.

Incydent w podmiocie publicznym - incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.

Incydent krytyczny –incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku prawnego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw lub wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT NASK.

2 Cel dokumentu

Celem dokumentu jest opisanie procedury reagowania na zaistniałe incydenty informatyczne związane z bezpieczeństwem.

Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność Urzędu.

3 Zakres stosowania

Procedurę należy stosować do wszystkich incydentów informatycznych związanych z bezpieczeństwem.

Realizacja wymogów procedury polega na stosowaniu się do zaleceń zawartych w procedurze.

Podstawą prawną do opracowania i wdrożenia dokumentu jest:

1. art. 22 ust.1 pkt 1 Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 05 lipca 2018 r
2. § 20 ust.2 pkt.13 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

4 Procedura

4.1 Zasady stosowania

Reagowanie na incydent powinno odbywać się jak najszybciej po zgłoszeniu. Z tego powodu wszyscy pracownicy obsługujący incydenty powinni znać treść niniejszej procedury i postępować zgodnie z jej zaleceniami.

4.2 Odpowiedzialność

1. Za poprawne przestrzeganie niniejszej procedury odpowiedzialny jest Administrator Systemu Informatycznego (ASI).
2. Osobą odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa zgodnie z art. 21 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa w Urzędzie jest Monika Bruch.

4.3 Reagowanie na awarię

1. Jeśli awaria dotyczy systemu krytycznego i może mieć wpływ na wydajność systemów teleinformatycznych, ASI informuje swojego bezpośredniego przełożonego.
2. W przypadku, gdy awarię można usunąć samodzielnie, to ASI dokonuje naprawy. Do podstawowych działań w takim wypadku zaliczyć możemy:
   a) wymianę stacji roboczej,
   b) wymianę podzespołów w stacji roboczej,
   c) wymianę urządzenia sieciowego,
   d) odtworzenie danych z kopii zapasowej.
3. Jeżeli ASI podejmie decyzję, iż nie może samodzielnie usunąć awarii, decyzję tę oraz wszelkie dodatkowe informacje dotyczące awarii eskaluje do producenta sprzętu lub oprogramowania. Jeżeli naprawa dotyczy sprzętu, producent naprawy dokonuje w obecności pracownika Urzędu. Jeżeli naprawa dotyczy oprogramowania (np. wersji BIOS), wgrywana poprawka powinna zostać pozytywnie zweryfikowana w środowisku testowym.
4. Jeśli istnieje powód wskazujący na to, że przyczyną awarii było naruszenie bezpieczeństwa, to ASI informuje bezpośredniego przełożonego. Dalej ma zastosowanie punkt 4.6 – reagowanie na naruszenie bezpieczeństwa niniejszej procedury.

4.4 Reagowanie na błędy w oprogramowaniu

1. Po otrzymaniu zgłoszenia dotyczącego wystąpienia błędu systemowego lub aplikacyjnego w oprogramowaniu, ASI diagnozuje przyczyny błędu oraz podejmuje działania zmierzające do rozwiązania problemu. Do podstawowych działań w tym zakresie możemy zaliczyć:
   a) wykorzystanie bazy wiedzy o błędach w oprogramowaniu,
   b) zmianę konfiguracji oprogramowania,
   c) ponowną instalację,
   d) instalację nowej wersji oprogramowania.
2. Jeżeli ASI nie może sam naprawić błędu w oprogramowaniu przekazuje do producenta oprogramowania (pracownik powinien w tym przypadku postępować zgodnie z umowami serwisowymi lub licencjami).
3. Jeśli istnieje powód wskazujący na to, że przyczyną błędu w oprogramowaniu było naruszenie bezpieczeństwa, to ASI informuje przełożonego.

4.5 Reagowanie na wykrycie złośliwego kodu

1. Po otrzymaniu zgłoszenia dotyczącego pojawienia się złośliwego kodu na stacji roboczej, serwerze, lub samodzielnemu wejściu w posiadanie wiedzy o takim zdarzeniu, ASI w pierwszej kolejności powinien:
   a) odłączyć komputer od sieci komputerowej,
   b) sprawdzić aktualność baz danych wirusów (jeśli są nieaktualne należy dokonać aktualizacji),
   c) sprawdzić poprawność działania oprogramowania antywirusowego (jeśli oprogramowanie nie działa poprawnie należy je odinstalować i zainstalować ponownie),
   d) uruchomić pełne skanowanie komputera i nośników informacji, z jakimi mógł mieć styczność,
2. Jeśli atak złośliwego kodu nie został zneutralizowany przez oprogramowanie antywirusowe to ASI nakazuje użytkownikowi przerwanie pracy. Następnie dokonuje ponownej instalacji systemu operacyjnego i oprogramowania oraz odzyskania danych z kopii zapasowych. Kopie zapasowe należy sprawdzić programem antywirusowym przed wgraniem do komputera.
3. Jeśli istnieje powód wskazujący na to, że przyczyną ataku złośliwego kodu było naruszenie bezpieczeństwa, to ASI informuje przełożonego.

4.6 Reagowanie na naruszenie bezpieczeństwa

1. **Kategorie incydentów**

1.1. Incydent bezpieczeństwa informacji oraz cyberbezpieczenstwa to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych oraz który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny. Jego przyczyną może być:

1.1.1. zdarzenie losowe zewnętrzne (np. klęski żywiołowe, pożary, zakłócenia w dostawie energii elektrycznej itp.), którego wystąpienie może spowodować zniszczenie lub uszkodzenie infrastruktury informatycznej albo dokumentacji papierowej oraz zakłócenie ciągłości pracy systemów nie powodując naruszenia poufności danych;

1.1.2. zdarzenie losowe wewnętrzne (np. błędy w oprogramowaniu , awarie sprzętu itp.), które mogą powodować zakłócenia ciągłości pracy systemów a także prowadzić do zniszczenia lub utraty danych;

1.1.3. świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych.

1.2. Incydentami bezpieczeństwa informacji w szczególności są:

1.2.1. naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;

1.2.2. naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;

1.2.3. naruszenie dostępności, to jest braku dostępu do danych przez uprawnionych użytkowników.

1.3. Przyczyny incydentów bezpieczeństwa informacji oraz cyberbezpieczeństwa mogą dotyczyć:

1.3.1. niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową;

1.3.2. działania szkodliwego oprogramowania;

1.3.3. próby omijania systemów zabezpieczeń;

1.3.4. nieautoryzowanego dostępu do systemów, aplikacji i dokumentów;

1.3.5. zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;

1.3.6. zniszczenia lub kradzieży nośników danych;

1.3.7. próby wyłudzeń informacji;

1.3.8. ataków socjotechnicznych , ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji;

1.3.9. nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;

1.3.10. naruszenia zasad obowiązujących w Urzędzie dotyczących bezpieczeństwa informacji, w tym danych osobowych.

2. Zgłaszanie incydentów związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem

2.1. W przypadku ujawnienia incydentu pracownik niezwłocznie powiadamia o tym fakcie Inspektora Ochrony Danych oraz Administratora Systemów Informatycznych. Zgłoszenie następuje poprzez ustanowione kanały komunikacji – telefonicznie, e-mail lub osobiście. Zgłoszenie należy następnie potwierdzić szczegółową notatką służbową, którą przekazuje się ASI oraz IOD poprzez swojego bezpośredniego przełożonego lub bezpośrednio w przypadku pracowników zatrudnionych na samodzielnych stanowiskach.

2.2. Notatka musi zawierać następujące informacje:

2.2.1. Imię i nazwisko osoby zgłaszającej;

2.2.2. stanowisko oraz komórka organizacyjna Urzędu;

2.2.3. dokładne miejsce oraz datę wystąpienia incydentu;

2.2.4. opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego.

2.3. Wzór notatki stanowi załącznik nr 1 do Instrukcji.

2.4. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.

3. Podejmowanie działań w związku ze zgłaszanymi incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem

3.1. Zgłoszenie incydentu rejestrowane jest przez ASI i przechowywane w teczce, wzór dziennika incydentów stanowi załącznik nr 2. Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.). Działania związane z obsługą zdarzenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia. W przypadku, kiedy zgłoszenie zakwalifikowane zostało jako incydent bezpieczeństwa informacji lub cyberbezpieczeństwa, dokonywana jest jego ocena istotności. Powyższe działania wykonuje ASI w porozumieniu z IOD.

3.2. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:

3.2.1. powstałe szkody będące wynikiem incydentu;

3.2.2. wpływ incydentu na działanie systemów;

3.2.3. wpływ incydentu na ciągłość działania Urzędu;

3.2.4. koszty usunięcia skutków incydentu;

3.2.5. szacowany czas naprawy skutków wywołanych incydentem;

3.2.6. oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.

3.3. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm" kończy postępowanie, o czym ASI informuje zgłaszającego.

3.4. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, ASI w porozumieniu z IOD podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.

3.5. Poinformowany o wynikach analizy incydentu oraz podjętych działaniach naprawczych ASI informuje Administratora.

3.6. W przypadku stwierdzenia incydentu w podmiocie publicznym lub incydentu krytycznego osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa nie później niż w ciągu 24 godzin od momentu wykrycia, zgłasza incydent do właściwego CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa - Państwowego Instytutu Badawczego ul. Kolska 12, 01-045 Warszawa).

3.7. Zgłoszenia do CSIRT NASK przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym https://incydent.cert.pl W przypadku braku możliwości przekazania go w sposób elektroniczny można zgłaszać przy użyciu innych dostępnych środków komunikacji (np. na numer telefonu +48223808274).

3.8. W zgłoszeniu przekazuje się informacje zgodnie z formularzem oraz zgodnie z treścią art. 23 ust. 1 Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 05 lipca 2018 r.

3.9. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa informacji oraz cyberbezpieczeństwa Administrator podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie, w zależności od wagi incydentu mogą być powiadomione organy ścigania.

4.7 Reagowanie na incydenty inne niż w procedurze

Po otrzymaniu zgłoszenia dotyczącego pojawienia się incydentu niesklasyfikowanego w niniejszej procedurze, ASI podejmuje decyzję o dalszym postępowaniu.

4.8 Reakcja na incydenty związane z naruszeniem bezpieczeństwa danych osobowych

Jeżeli zostaje stwierdzone naruszenie ochrony danych osobowych realizowane są działania zgodnie z Polityką Ochrony Danych.

4.9 Zmiana klasyfikacji zgłoszenia

Na każdym z etapów postępowania z incydentem należy zwracać uwagę na odpowiednią jego klasyfikację. Klasyfikację incydentu należy zmienić jeśli w trakcie prac incydent zostanie inaczej zdiagnozowany.

Załącznik nr 1

Zgłaszanie incydentów związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem – wzór notatki służbowej ze zgłoszeniem

Imię i nazwisko osoby zgłaszającej .....

Stanowisko oraz komórka organizacyjna.....

Dokładne miejsce oraz data wystąpienia incydentu

.....

.....

Opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego

.....

.....

.....

.....

.....

Procedura reagowania na incydenty		
Wersja: 1.0	Data wprowadzenia:	28.10.2021

LP.	DATA ZGŁOSZENIA	OSOBA ZGŁASZAJĄCA	KATEGORIA INCYDENTU	DATA WYSTĄPIENIA	PODJĘTE DZIAŁANIA	ZGŁOSZENIE DO CSIRT NASK
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						