Warszawa, dnia 28 lutego 2022 r.

Poz. 15

Z A R Z Ą D Z E N I E

M I N I S T R A F I N A N S Ó W

z dnia 24 lutego 2022 r.

w sprawie wprowadzenia Polityki Zarządzania Ciągłością Działania

Na podstawie art. 34 ust. 1 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2021 r. poz. 178, 1192, 1535 i 2105) zarządza się, co następuje:

§ 1. 1. Wprowadza się Politykę Zarządzania Ciągłością Działania, zwaną dalej „Polityką", stanowiącą załącznik do zarządzenia, w:

1) Ministerstwie Finansów;
2) izbach administracji skarbowej;
3) urzędach skarbowych;
4) urzędach celno-skarbowych wraz z podległymi oddziałami celnymi;
5) Krajowej Informacji Skarbowej;
6) Krajowej Szkole Skarbowości;
7) Centrum Informatyki Resortu Finansów;
8) delegaturach jednostek organizacyjnych Krajowej Administracji Skarbowej utworzonych przez ministra właściwego do spraw finansów publicznych na podstawie art. 36 ust. 2 ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. z 2021 r. poz. 422, z późn. zm.[1)]).

2. Polityki nie stosuje się do działalności związanej z informacjami niejawnymi, które regulują przepisy odrębne.

§ 2. 1. Politykę stosuje się w celu utworzenia systemu zarządzania ciągłością działania w jednostkach, o których mowa w ust. 1, zgodnie z wymaganiami międzynarodowych norm PN-EN ISO 22301:2020 Bezpieczeństwo i odporność. Systemy zarządzania ciągłością działania. Wymagania

---

1) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2021 r. poz. 464, 694, 802, 815, 954, 1005, 1718, 2076 i 2105.

oraz PN-EN ISO 22313:2020 Bezpieczeństwo i odporność - Systemy zarządzania ciągłością działania – Wytyczne dotyczące stosowania ISO 22301.

2. System zarządzania ciągłością działania ma na celu przygotowanie jednostek, o których mowa w ust. 1, do zabezpieczenia się przed negatywnym wpływem zakłóceń, które mogą pojawić się w ich funkcjonowaniu, i pozwoli na nieprzerwane realizowanie procesów krytycznych tych jednostek oraz minimalizowanie strat wywołanych tymi zakłóceniami.

§ 3. Zarządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Minister Finansów wz.: A. Soboń

Załącznik do zarządzenia Ministra Finansów
z dnia 24 lutego 2022 r. w sprawie wprowadzenia
Polityki Zarządzania Ciągłością Działania
(poz. 15)

POLITYKA ZARZĄDZANIA CIĄGŁOŚCIĄ DZIAŁANIA

1. Wstęp

Zarządzanie ciągłością działania to kompleksowe działania pozwalające zidentyfikować potencjalne zagrożenia i określić ich wpływ na organizację. Mają one na celu budowanie odporności i zdolności organizacji do efektywnej reakcji na zagrożenie tak, aby zabezpieczyć realizację zadań organizacji i jej wizerunek.

Celem Polityki jest przedstawienie podejścia do ustanowienia i wdrożenia mechanizmów zabezpieczających przed zagrożeniami wpływającymi na ciągłość realizacji procesów oraz na wizerunek jednostek[1)], czyli systemu zarządzania ciągłością działania, zwanego dalej „Systemem".

Polityka określa:

1) elementy i etapy wdrażania Systemu;

2) działania niezbędne do utworzenia i doskonalenia Systemu, mające na celu opracowanie i wdrożenie rozwiązań pozwalających na utrzymanie funkcjonowania organizacji.

2. Obowiązki

Każdy pracownik[2)] jest odpowiedzialny za utrzymanie właściwego poziomu gotowości do zapewnienia funkcjonowania jednostki w zakresie swoich obowiązków i uprawnień.

Obowiązki w zakresie wdrożenia, koordynowania i monitorowania oraz nadzoru nad poprawnością funkcjonowania Systemu realizują:

- Departament Bezpieczeństwa i Ochrony Informacji w Ministerstwie Finansów,
- komórki do spraw bezpieczeństwa i ochrony informacji znajdujące się w izbach administracji skarbowej,
- komórka organizacyjna Krajowej Informacji Skarbowej, która odpowiada za realizowanie, koordynowanie i nadzór nad realizacją zadań z zakresu zarządzania ciągłością działania,

---

1) Jednostki wymienione w § 1 ust. 1 zarządzenia.

2) Przez pracownika rozumie się kierującego jednostką, osobę fizyczną zatrudnioną na podstawie umowy o pracę, powołania, mianowania albo umowy cywilnoprawnej, osobę pełniącą w niej służbę, w tym funkcjonariusza Służby Celno-Skarbowej, oraz praktykanta, stażystę lub wolontariusza.

- komórka organizacyjna Krajowej Szkoły Skarbowości, która odpowiada za realizowanie, koordynowanie i nadzór nad realizacją zadań z zakresu zarządzania ciągłością działania.

Obowiązki w zakresie utrzymania i doskonalenia Systemu spoczywają na pracownikach, którzy realizują zadania wynikające z przypisanych ról i zadań określonych w opracowanej dokumentacji Systemu.

3. Elementy i etapy działań związane z wdrażaniem Systemu

Do wdrożenia w organizacji Systemu niezbędna jest realizacja następujących działań:

1) określenie ról poszczególnym pracownikom i przypisanie im zadań i odpowiedzialności w Systemie;
2) identyfikacja procesów i powiązań pomiędzy nimi oraz wyszczególnienie procesów głównych i procesów pomocniczych organizacji;
3) analiza BIA – identyfikacja procesów krytycznych[3)];
4) analiza ryzyka dla procesów krytycznych;
5) strategia ciągłości działania;
6) plany ciągłości działania.

System powinien docelowo obejmować całą jednostkę, natomiast dopuszczalne jest, by działania związane z jego wdrożeniem rozpocząć od obszaru wskazanego przez kierującego jednostką.

3.1. Role

Tworząc System, należy wskazać osoby i zespoły odpowiedzialne za wdrożenie, utrzymanie i doskonalenie Systemu oraz wyznaczyć im role, zadania, zakresy obowiązków i odpowiedzialności.

Polityka nie narzuca jednolitych rozwiązań w zakresie wyznaczania ról, zadań, obowiązków i odpowiedzialności, uwzględniając różnorodność jednostek, ich zadań i struktur organizacyjnych.

Określenie ról wynikających z Systemu i przypisanie do nich osób należy wskazać w opracowywanej dokumentacji Systemu.

3.2. Identyfikacja procesów

Wdrażanie Systemu związane jest z opisaniem działalności jednostki, którą należy przedstawić za pomocą zidentyfikowania i opisania realizowanych w niej procesów.

---

[3] Proces krytyczny – proces główny, który powinien być realizowany w sposób ciągły i niezakłócony, a którego przedłużająca się, nieplanowana przerwa w realizacji spowodowałaby negatywne skutki finansowe, prawne lub wizerunkowe

Procesy dzieli się na procesy główne, do realizacji których organizacja została powołana, i procesy pomocnicze, zapewniające zasoby do działania procesów głównych.

3.3. Analiza BIA

Po zidentyfikowaniu procesów realizowanych w jednostce należy określić jakie procesy są dla organizacji krytyczne i w tym celu wykonuje się analizę BIA – analiza wpływu biznesowego (business impact analysis), która:

1) pozwoli na zidentyfikowanie krytycznych procesów i zasobów niezbędnych do utrzymania bądź wznowienia tych procesów, a także na określenie skutków przerwania tych procesów w określonych przedziałach czasowych;

2) określi kluczowe wskaźniki RTO[4)] – Recovery Time Objective i RPO[5)] – Recovery Point Objective.

Analizę BIA przeprowadza się zgodnie z zasadami opisanymi w normie ISO/TS 22317:2015 – Bezpieczeństwo społeczne – Systemy zarządzania ciągłością działania – Wytyczne do analizy wpływu na biznes (BIA).

3.4. Analiza ryzyka

Analiza ryzyka jest to działanie polegające na analizowaniu informacji do zidentyfikowania źródeł ryzyka oraz jego oszacowania. W kontekście ciągłości działania analiza ryzyka przeprowadzana jest dla procesów krytycznych i koniecznych do ich realizacji zasobów.

Analiza ryzyka określa wpływ potencjalnego zagrożenia na jednostkę oraz stworzenie warunków do budowania odporności i zdolności skutecznej reakcji w zakresie:

- ochrony interesów Skarbu Państwa,
- gwarancji płynności realizowanych procesów,
- minimalizowania strat związanych z przywracaniem realizacji procesów bądź odtwarzaniem utraconych zasobów,
- zarządzania wizerunkiem jednostki,
- unikania lub minimalizowania konsekwencji prawnych wynikających z niewykonania obowiązujących przepisów.

---

4) Przez RTO rozumie się wymagany czas odtworzenia procesu, czyli czas, w jakim należy wznowić proces przerwany w wyniku zakłócenia działalności.

5) Przez RPO rozumie się punkt odtworzenia danych, czyli akceptowalny poziom utraty danych wyrażony w czasie, po przekroczeniu którego realizacja procesu będzie niemożliwa lub poważnie zakłócona.

Analiza ryzyka pomaga w:

1) zaplanowaniu i wdrożeniu działań i rozwiązań zapobiegawczych, ograniczających prawdopodobieństwo wystąpienia zagrożenia;

2) określeniu na podstawie zebranych danych poziomu ryzyka związanego z niedostępnością poszczególnych grup zasobów, nadanie im priorytetów oraz opracowanie planu minimalizacji ryzyka dla poszczególnych zasobów.

Precyzyjne określenie wpływu poszczególnych zagrożeń na ciągłość procesów krytycznych, a także zdefiniowanie scenariuszy zdarzeń, umożliwia usystematyzowanie już posiadanych lub wdrożenie brakujących rozwiązań proceduralnych, organizacyjnych i technicznych w zakresie ciągłości działania, adekwatnych do skali prawdopodobnych zdarzeń. Scenariusze zdarzeń definiują najbardziej dotkliwe oraz prawdopodobne zagrożenie, które w momencie wystąpienia może doprowadzić do całkowitego przerwania realizacji procesów krytycznych i służą do opracowania strategii zachowania ciągłości działania.

Zasady zarządzania ryzykiem, porady w zakresie szacowania ryzyka, postępowania z ryzykiem, akceptacji ryzyka, informowania o ryzyku i przeglądu ryzyka określa norma PN-ISO 31000:2018 Zarządzanie ryzykiem – Zasady i wytyczne.

3.5. Strategia ciągłości działania

Celem strategii ciągłości działania jest:

1) określenie sposobu zabezpieczenia i odtworzenia krytycznych procesów oraz zasobów wymaganych do ich realizacji;

2) wskazanie najbardziej skutecznych środków zapobiegawczych koniecznych do zachowania ciągłości działania jednostki w sytuacji wystąpienia zagrożenia.

Strategia ciągłości działania określa sposób postępowania z zasobami niezbędnymi do realizacji procesów krytycznych, w szczególności z zasobami:

- ludzkimi,
- informatycznymi,
- rzeczowymi.

Do realizacji procesów krytycznych w sytuacji wystąpienia zagrożenia wykorzystuje się zasoby dostępne w jednostce i funkcjonujące już rozwiązania. W szczególnych sytuacjach możliwe jest wykorzystanie zasobów dostępnych na podstawie zawartych umów z podmiotami zewnętrznymi.

3.6. Plan ciągłości działania

Dla procesów krytycznych opracowuje się plany ciągłości działania zapewniające w sytuacji wystąpienia zagrożenia zachowanie ciągłości ich realizacji na określonym poziomie lub w celu przywrócenia ich działania w określonym czasie. Procesy pomocnicze ujmuje się w tych planach w zakresie, w jakim wpływają na krytyczne procesy główne.

Plan ciągłości działania określa:

1) szczegółowy sposób postępowania w przypadku wystąpienia zagrożenia;

2) osoby wskazane do realizacji poszczególnych działań;

3) zasoby niezbędne do funkcjonowania procesów krytycznych;

4) rozwiązania organizacyjne wspomagające realizację procesów krytycznych.

Sposób postępowania opisany w planie ciągłości działania polega na:

1) określeniu czynności gwarantujących zachowanie ciągłości działania i czasów ich wykonania;

2) ograniczeniu przypadkowych czynności i decyzji, w celu ograniczeniu błędów, zaniedbań lub powielania czynności;

3) określeniu procedur przywracania pełnej działalności jednostki.

Dopuszcza się włączenie do Systemu rozwiązań doraźnych w formie awaryjnych planów ciągłości działania opracowanych w związku z wystąpieniem niespodziewanych zdarzeń.

4. Utrzymanie i doskonalenie Systemu

Funkcjonowanie Systemu zależne jest od opracowanych i wdrożonych rozwiązań z zakresu ciągłością działania, jak również od innych przyjętych w jednostce rozwiązań dotyczących, w szczególności:

1) bezpieczeństwa teleinformatycznego;

2) bezpieczeństwa informacji;

3) bezpieczeństwa fizycznego;

4) zarzadzania kryzysowego;

5) ochrony danych osobowych.

Zaleca się, prowadzenie i weryfikowanie aktualności dokumentacji jednostki, która może wpływać na bezpieczeństwo, uodpornienie na zagrożenia i zapewnienie prawidłowego funkcjonowania, w powiązaniu z dokumentacją Systemu, w szczególności planu zarządzania kryzysowego, procedur

postępowania, instrukcji, planów awaryjnych dla systemów teleinformatycznych, planów ochrony obiektu.

Celem działań weryfikacyjnych jest potwierdzenie:

1) spójności planów ciągłości działania;

2) aktualności przyjętych rozwiązań;

3) zgodności z obowiązującą w jednostce dokumentacją z zakresu ciągłości działania.

4.1. Testowanie planów ciągłości działania

Podstawowym narzędziem weryfikacji poprawności funkcjonowania Systemu jest cykliczne testowanie rozwiązań zawartych w planach ciągłości działania. Testy dostarczają wiarygodnych informacji zarządczych o stanie Systemu w jednostce, w szczególności ocenę:

- adekwatności planów ciągłości działania do zmieniających się procesów i otoczenia jednostki;
- czy plany ciągłości działania pozwalają na minimalizację ryzyka możliwego zagrożenia.

Testy obejmują wszystkie zdefiniowane plany ciągłości działania w jednostce i zaangażowanie wszystkich niezbędnych zasobów do realizacji procesów krytycznych wraz z niezbędnymi rozwiązaniami organizacyjnymi, technologicznymi, infrastrukturą i danymi.

Poszczególne testy mogą dotyczyć tylko wybranych części planu ciągłości działania, w szczególności:

1) określonej operacji;

2) określonej procedury;

3) komunikacji wewnętrznej.

W wybranych zakresach działania jednostki testy powinny być przeprowadzane co najmniej raz w roku na podstawie opracowanych scenariuszy testowych.

Scenariusze testowe należy regularnie przeglądać pod kątem:

1) aktualności planów ciągłości działania;

2) zidentyfikowanych zagrożeń;

3) możliwości doskonalenia Systemu;

4) minimalizacji skutków wystąpienia zakłócenia.

Wykonanie testu planu ciągłości działania zostaje potwierdzone raportem, zawierającym jego wyniki. Raport stanowi syntetyczne podsumowanie przeprowadzonych działań i przedstawia ocenę

skuteczności Systemu. Raport wskazuje również potrzebne działania korygujące, z podziałem na działania usprawniające i naprawcze.

Rekomendacje działań korygujących zawierają uzasadnienie, są skierowane do właściwych osób i weryfikowane jest ich wprowadzenie.

4.2. Doskonalenie i aktualizacja Systemu

System musi być utrzymywany w sprawności, stale aktualizowany i doskonalony w celu zapewnienia jego funkcjonowania oraz dostosowania do zagrożeń. Zadania te są realizowane przy udziale komórek i osób zaangażowanych w realizację określonych procesów krytycznych jednostki, dla których opracowane są rozwiązania z zakresu ciągłości działania. Celem aktualizacji i doskonalenia Systemu jest zwiększenie prawdopodobieństwa zapewnienia nieprzerwanej realizacji procesów krytycznych.

Aktualizacji Systemu dokonuje się w przypadku:

1) zmiany wykazu procesów jednostki, w szczególności w związku ze zmianą realizowanych zadań;
2) zmiany sposobu realizacji procesów krytycznych objętych planami ciągłości działania;
3) zmiany struktury organizacyjnej;
4) zmiany struktury zarządzania ciągłością działania;
5) zmiany systemów informatycznych używanych do realizacji procesów krytycznych;
6) zmiany siedziby;
7) zmiany dostawców usług i partnerów zewnętrznych;
8) wystąpienia zakłócenia skutkującego uruchomieniem planu ciągłości działania;
9) wydania rekomendacji po przeprowadzeniu testów albo przeglądu.

Aktualizacja i doskonalenie Systemu poprzedzone są jego przeglądem. Przegląd Systemu ma na celu sprawdzenie, czy System jest spójny i czy zawiera odpowiednie zabezpieczenia do postępowania z ryzykiem. Na podstawie przeglądu wytypowanych obszarów Systemu, określa się:

1) poprawność identyfikacji procesów krytycznych;
2) poprawność identyfikacji i klasyfikacji zakłóceń i ich wpływu na działalność;
3) adekwatność działań podmiotów zaangażowanych w System i struktur zarządzania ciągłością działania;
4) efektywność w osiągnięciu celów Systemu, w tym poprawność określenia czasu odtworzeniowego RTO;

5) wiedzę i doświadczenie pracowników w zakresie realizacji zadań wynikających z planów ciągłości działania;

6) efektywność wprowadzonych rekomendowanych zmian;

7) czy poprzednio wskazane rekomendacje zostały wprowadzone i usunięte uchybienia;

8) czy przeprowadzono testy.

5. Szkolenia

Szkolenia pracowników w zakresie wiedzy o Systemie zwiększają prawdopodobieństwo niezakłóconej realizacji zadań, za które pracownicy odpowiadają. Szkolenia powinny obejmować wszystkich pracowników, ze szczególnym uwzględnieniem pracowników, którzy uczestniczą w realizacji zadań wynikających z planów ciągłości działania. Wskazany jest podział szkoleń ze względu na następujące grupy pracowników, do których jest kierowany, na szkolenie:

1) ogólne kierowane do wszystkich pracowników;

2) specjalistyczne kierowane do osób pełniących określone role w strukturze zarządzania ciągłością działania, w tym osób które realizują zadania wynikające z obowiązków zapisanych w opracowanej dokumentacji z obszaru ciągłości działania;

3) dla kadry kierowniczej[6)] różnego szczebla prowadzące do uświadomienia znaczenia i konieczności zaangażowania w działania z obszaru ciągłości działania oraz odpowiedzialności jaką ponoszą osoby zarządzające pracownikami w organizacji.

6. Opracowanie dokumentacji Systemu

Departament Bezpieczeństwa i Ochrony Informacji w Ministerstwie Finansów opracuje w porozumieniu z jednostkami wzorcową dokumentację i instrukcje dla jednostek w zakresie wdrożenia Systemu. Dokumentacja ta podlegać będzie zmianom w zależności od potrzeb i wymagań zgłaszanych przez jednostki. Opracowane instrukcje dotyczyć będą w szczególności:

1) ról w Systemie;

2) analizy BIA – identyfikacji procesów krytycznych;

3) analizy ryzyka dla procesów krytycznych;

4) strategii ciągłości działania;

5) planów ciągłości działania;

6) scenariuszy testów i raportów z przeprowadzonych testów i przeglądów.

---

6) Przez kadrę kierowniczą rozumie się osoby kierujące jednostką lub komórką organizacyjną.