Zarządzenie nr 2/2021
z dnia 18.01.2021 r.
Dyrektora
Zespołu Szkól i Placówek w Wołkowyi

w sprawie wprowadzenia „Planu ciągłości działania na wypadek dysfunkcji systemu teleinformatycznego w Zespole Szkół i Placówek w Wołkowyi”

Na podstawie: art. 20 ust.2 pkt 1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r. poz. 526) zarządzam, co następuje:

§ 1

Wprowadzam: „Plan ciągłości działania na wypadek dysfunkcji systemu teleinformatycznego w Zespole Szkół i Placówek w Wołkowyi” stanowiący Załącznik nr 1 do niniejszego zarządzenia,

§ 2

Wykonanie zarządzenia w/w zakresie oraz wprowadzenia w życie powierza się Administratorowi Systemu Informatycznego oraz Inspektorowi Ochrony Danych Osobowych.

§ 2

Zarządzenie wchodzi w życie z dniem 18.01.2021 r.

.

Dyrektor
Zespołu Szkół i Placówek w Wołkowyi

mgr Witold Orłowski

załącznik nr 1 do Zarządzenie nr 1/2021

Plan ciągłości działania
na wypadek
dysfunkcji systemu teleinformatycznego
w Zespole Szkół i Placówek w Wołkowyi

…….....…… …….....…….

/opracował/ */zatwierdził/*

1. CEL PROCEDURY

Celem Procedury jest minimalizacja zakłóceń w realizacji działalności statusowej Zespołu Szkół i Placówek w Wołkowyi, w związku z dysfunkcją systemu sieciowego.

2. PRZEDMIOT

Przedmiotem procedury jest postępowanie w przypadku zaistnienia zdarzeń mających wpływ (również potencjalny) na bezpieczeństwo informacji oraz ciągłość działania w Zespole Szkół i Placówek w Wołkowyi.

3. ZAKRES STOSOWANIA

Zdefiniowanie działań koniecznych do podjęcia w przypadku dysfunkcji systemu informatycznego.

4. ODPOWIEDZIALNOŚĆ I UPRAWNIENIA

Za opracowanie i utrzymanie niniejszego planu ciągłości działania odpowiedzialny jest głównie Pracodawca oraz Administrator Systemów Informatycznych i Inspektor Ochrony Danych Osobowych.

Za nadzór nad realizacją działań związanych z opracowaniem i utrzymaniem niniejszego planu ciągłości działania odpowiedzialny jest Administrator Danych Osobowych (pracodawca), Administrator Systemów Informatycznych oraz Inspektor Ochrony Danych Osobowych.

Za realizację działań przewidzianych w niniejszym planie ciągłości działania odpowiedzialne są wskazane w nim osoby.

5. OPIS POSTĘPOWANIA

5.1. WARUNKI URUCHOMIENIA PLANU

Plan uruchamiany jest w przypadku dysfunkcji systemu teleinformatycznego, mającego wpływ na ciągłość działania Zespołu Szkół i Placówek w Wołkowyi.

5.2. OSOBY ORAZ ZASOBY WYMAGANE DO REALIZACJI PLANU

O uruchomieniu planu decyduje Dyrektor szkoły (ADO) lub osoby upoważnione przez Dyrektora, w porozumieniu z Administratorem Systemów Informacji (ASI) oraz Inspektorem Ochrony Danych Osobowych (IODO).

6. DZIAŁANIA ZAPEWNIAJĄCE PRZYWRÓCENIE ZDOLNOŚCI REALIZACJI FUNKCJONOWANIA SYSTEMÓW TELEINFORMATYCZNYCH

Lp.	Funkcja	Opis działań	Potrzebne zasoby/ osoby odpowiedzialne
1.	Zweryfikować zasadność zgłoszenia od użytkownika	Sprawdzić, czy zgłoszenie dotyczy zdarzenia spowodowanego awarią systemu informatycznego.	Zapewnić: - dostęp do infrastruktury informatycznej na stanowisku, skąd pochodzi zgłoszenie. Odpowiedzialny: ASI
2.	Zweryfikować zasadność zgłoszenia od ucznia/ rodzica	Sprawdzić, czy zgłoszenie dotyczy zdarzenia spowodowanego awarią systemu informatycznego, awarią sprzętu komputerowego, awarią systemu operacyjnego, itp.	Zapewnić: kontakt z nauczycielem prowadzącym zajęcia, wychowawcą, ASI (informatykiem), Administratorem (usługodawcą) systemu informacyjnego - VULCAN
3.	Ustalić źródła awarii- zidentyfikować źródła po stronie użytkownika (nauczyciel, uczeń, szkoła)	Ustalić, co jest przyczyną awarii: - przerwa w zasilaniu prądem, - brak połączenia z siecią Internet, - wadliwe działanie sprzętu, - wadliwe działanie aplikacji, - wadliwe działanie systemu, na którym uruchomiona jest	Zapewnić: - kontakt z nauczycielem/wychowawcą, kontakt z ASI, - dostęp do serwerowni oraz do sprzętu, który uległ awarii, - w przypadku awarii zasilania elektrycznego wezwać elektryka, - powiadomić OSE - powiadomić Pogotowie Energetyczne.

		aplikacja.	
4.	Określić skalę awarii	Ustalić, czy awaria powoduje zatrzymanie pracy: - jednego stanowiska pracy lub całej szkoły, całego systemu połączenia zdalnego	Zapewnić: - kontakt z kluczowymi pracownikami, osobami odpowiedzialnymi za utrzymanie usług zewnętrznych w czasie realizacji usług lekcji zdalnych) Odpowiedzialny: dyrektor szkoły, ASI
5.	Ustalić czy wznawianie usługi może odbywać się w dotychczasowej lokalizacji	Działanie ma na celu zweryfikowanie, czy wznawiane usługi uruchamiane będą w dotychczasowej lokalizacji, czy w lokalizacjach alternatywnych.	Zapewnić: - możliwość uruchomienia dowolnych usług w lokalizacji: - infrastrukturę sieciową, - zasilanie prądem Odpowiedzialni: ASI, konserwator.
6.	Zakupić niezbędne elementy wyposażenia, dokonać naprawy (wymiany) urządzeń uruchomić aplikację	W przypadku braku możliwości zakupu należy znaleźć rozwiązanie alternatywne (np. zdecydować o przeniesieniu aplikacji na stałe na inny serwer)	Zapewnić: - środki na zakup elementów niezbędnych do ponownego uruchomienia systemu. Odpowiedzialny: Dyrektor szkoły, ASI
7.	Zweryfikować możliwość przeniesienia aplikacji na inny serwer	Sprawdzić, czy aplikacja może być uruchomiona na którymś z działających poprawnie serwerów.	Odpowiedzialny: ASI
8.	Przygotować serwer	Jako serwer zastępczy można wykorzystać np. Komputer typu	Odpowiedzialny: ASI

	zastępczy	desktop w z dyskami w macierzy RAID 1. (MIRROR), który należy odpowiednio skonfigurować. Po uruchomieniu aplikacji na serwerze zastępczym należy przetestować jej działanie.	
9.	Podjąć decyzję o terminie odtworzenia maszyny	W razie konieczności należy skontaktować się z właściwymi osobami utrzymującymi sieć i dane w chmurze.	Odpowiedzialny: ASI
10.	Przywrócić funkcjonowanie aplikacji / systemu	Spróbować usunąć przyczynę nieprawidłowego działania. W razie konieczności należy odtworzyć aplikację korzystając z kopii zapasowych (także tych, udostępnianych przez usługodawcę).	Zapewnić: - dostęp do najbardziej aktualnej wersji aplikacji, - dostęp do aktualnej bazy danych. Odpowiedzialny: ASI
11.	Sprawdzenie aplikacji / systemu	Po przeniesieniu / uruchomieniu należy zweryfikować prawidłowe funkcjonowanie aplikacji / systemów zainstalowanych na serwerze/ komputerach stacjonarnych, przenośnych.	Odpowiedzialny: ASI
12.	Uruchomienie usługi w systemie informatycznym Szkoły	Po uruchomieniu usługi o tym fakcie należy powiadomić wszystkie osoby, które utraciły dostęp do systemu	Wznowienie działania usługi, możliwie na nowej maszynie lub z wykorzystaniem nowej usługi (chmura).
13.	Sytuacja krytyczna (opcjonalnie)	W sytuacji krytycznej, po uruchomieniu agregatu prądu (jeżeli będzie taka konieczność) należy zapewnić dostęp do sieci informatycznej – poczta, strony www,	Odpowiedzialny: dyrektor szkoły, ASI

		programy kluczowe ze względu na utrzymanie ciągłości działania Szkoły, TYLKO pracownikom realizującym działania strategiczne.	

7. TESTOWANIE PLANU

L.p.	Opis testu	Termin realizacji	Oczekiwany wynik	Odpowiedzialny
1.	Symulacja wyłączenia serwera danej aplikacji, brak możliwości wykonywania usług, symulacja na podstawie scenariusza zawartego w protokole.	1 dzień roboczy – lub czas wykonania testu (Nie dłużej niż 1 dzień roboczy)	Wznowienie działania usługi, możliwie na nowej maszynie (opcjonalnie)	ASI

8. SZKOLENIE DLA UCZESTNIKÓW PLANU

Uczestnicy planu są zapoznawani z jego treścią każdorazowo przed przeprowadzeniem jego testowania.

9. AKTUALIZACJA PLANU

Plan aktualizowany jest każdorazowo w przypadku zmian kadrowych oraz w przypadku niepowodzenia w jego testowaniu.

REGULAMIN OKREŚLAJĄCY ZASADY I PROCEDURY KORZYSTANIA Z LEGALNEGO OPROGRAMOWANIA, SPRZĘTU KOMPUTEROWEGO I SIECI KOMPUTEROWEJ W ZESPOLE SZKÓŁ I PLACÓWEK W WOŁKOWYI

I. Zasady korzystania z oprogramowania.

1. Zobowiązuję pracowników do korzystania z legalnego oprogramowania.
2. Szczególne uregulowania w bieżącej pracy pracowników dotyczące ochrony własności intelektualnej są wyrażone w niniejszym regulaminie.
3. Wszyscy pracownicy jednostki mogą wykorzystywać jedynie legalne oprogramowanie, za które odpowiedzialny jest zarządzający oprogramowaniem.
4. Instalacje oprogramowania na stanowiskach komputerowych mogą być dokonywane z nośników znajdujących się w zasobach jednostki. Ich instalacja może być dokonywana wyłącznie przez Administratora Systemów Informatycznych lub przez osoby przez nich upoważnione do przeprowadzenia instalacji autoryzowanej.
5. Pracownik może dokonać tylko autoryzowanej instalacji autoryzowana instalacja następuje po wydaniu zgody przez informatyka, zinwentaryzowaniu oprogramowania i dopisaniu go do karty oprogramowania komputera.
6. Oprogramowanie w wersjach testowych lub w jakikolwiek inny sposób ograniczone umowami licencyjnymi może być użytkowane wyłącznie zgodnie z jego przeznaczeniem i w czasie określonym w umowie licencyjnej.
7. Wszyscy pracownicy zobowiązują się do przestrzegania wymogu pracy wyłącznie na oprogramowaniu zainstalowanym przez Administratora Systemów Informatycznych, zleconych przez Administratora Danych Osobowych (pracodawcę).
8. Pracownicy otrzymują wyraźny zakaz wnoszenia na teren zakładu pracy prywatnych kopii oprogramowania oraz plików multimedialnych. Zabrania się pobierania i kopiowania z Internetu wszelkich utworów (programów komputerowych, utworów muzycznych, filmów, gier komputerowych, itp.), będących przedmiotem ochrony praw autorskich.
9. Naruszenia wyżej wymienionych ustaleń, ze względu na obowiązujące przepisy prawne, stanowią poważne naruszenie dyscypliny pracy.
10. Każdy z pracowników zobowiązany jest podpisać porozumienie z pracodawcą stanowiące załącznik nr 4 do niniejszego Zarządzenia, zobowiązując się do przestrzegania zasad i procedur wynikających z Porozumienia.
11. Porozumienie wymienione w ust. 10 podpisywane jest nie później niż w ciągu 7 dni od dnia podjęcia zatrudnienia lub czynności w jednostce i przechowywane w dokumentacji ochrony danych osobowych.

II. Zasady korzystania ze sprzętu komputerowego.

1. Zabrania się dokonywania bez zgody Administratora Systemów Informatycznych zmian w ustawieniach systemowych komputerów, w szczególności: ustawień BIOS-u, ustawień systemu operacyjnego (w tym instalowania urządzeń), ustawień sieci komputerowej.
2. Zabrania się samodzielnego otwierania obudowy komputera oraz innych części komputerowych (np. monitorów, drukarek, myszy).
3. Uprawnionymi do dokonywania czynności, o których mowa w ust. 2, na warunkach określonych warunkami gwarancji sprzętu, jest informatyk.
4. Pracownik, w którego dyspozycji pozostaje komputer ma obowiązek wyłączyć go po zakończeniu pracy.
5. Korzystanie z nośników danych dopuszczalne jest po wcześniejszym sprawdzeniu ich programem antywirusowym.
6. Pracownik ma prawo bez wiedzy i zgody Administratora Systemów Informatycznych:
   - wymienić toner, tusz, taśmę, (materiały eksploatacyjne) itp.,
   - usunąć zakleszczony papier.
7. Zezwala się pracownikom na korzystanie z przenośnego komputera służbowego poza miejscem pracy, pod warunkiem przestrzegania „Procedury użytkowania komputerów przenośnych".
8. Wszyscy pracownicy jednostki korzystający z komputerów przenośnych mogą korzystać z nich poza miejscem pracy zachowując obowiązujące w jednostce zasady korzystania z oprogramowania.
9. Zabrania się użyczania komputerów osobom postronnym.
10. Naruszenia wyżej wymienionych ustaleń, ze względu na obowiązujące przepisy prawne, stanowią poważne naruszenie dyscypliny pracy.

Procedury kontrolne dotyczące komputerowego stanowiska pracy.

1. Wprowadza się obowiązek kontrolny zawartości komputerów stanowiących własność jednostki wykorzystywanych przez pracowników, dla zapewnienia ochrony zasobów teleinformatycznych i danych. Automatyczne procedury sprawdzające komputerów pracowników nadzoruje Administrator Bezpieczeństwa Informacji oraz Inspektor Ochrony Danych Osobowych.
2. Procedury sprawdzające realizowane są przy pomocy specjalistycznego oprogramowania, którego raporty stanowią podstawę dla działań naprawczych podejmowanych przez Administrator Bezpieczeństwa Informacji oraz Inspektora Ochrony Danych Osobowych.
3. Ruch w sieci teleinformatycznej, generowany przez pracownika, podlega monitoringowi z automatycznym zapisem dostępów do stron www.
4. Informacje statystyczne potwierdzające: adresy sieciowe, czas dostępu do najczęściej odwiedzanych przez pracowników serwisów internetowych, gromadzonych plików oraz uruchamianych aplikacji mogą:
   - podlegać analizie i przekazania do Kierowników komórek organizacyjnych,
   - stanowić podstawę do dalszych kroków podejmowanych na drodze służbowej.

Katalog działań specjalnych, dozwolonych dla Administratora Sieci Informatycznej i Inspektora Ochrony Danych Osobowych.

Niektóre działania zabronione, mogą być wykonywane w przypadku:

1. realizacji działań zgodnych z zakresem obowiązków, dyspozycją przełożonego lub przepisami szczególnymi obowiązującymi pracowników,
2. prowadzenia interakcji z internetowymi portalami instytucji, urzędów, organizacji, w celu realizacji zadań czy wykonywania obowiązków,
3. uzyskaniem pisemnej zgody Dyrektora szkoły,
4. realizacji na rzecz jednostki, poprzez osoby trzecie, zapisów umów, zwłaszcza, gdy niezbędne jest ustanowienie interoperacyjności pomiędzy systemami teleinformatycznymi wewnętrznymi i systemami zewnętrznymi.

POROZUMIENIE

Niniejsze porozumienie (zwane dalej „Porozumieniem") zostało zawarte w dniu …… r. w Wołkowyi pomiędzy: Zespołem Szkół i Placówek w Wołkowyi (zwanym dalej „Pracodawcą"), reprezentowanym przez Dyrektora Szkoły, Witolda Orłowskiego a Panią/Panem ....., zwaną/nym dalej „Pracownikiem".

1. Pracownik zatrudniony jest przez Pracodawcę na podstawie umowy o pracę\zlecenia*.
2. Pracodawca wyposażył stanowisko pracy Pracownika w oprogramowanie komputerowe zgodne z wykonywaną pracą.
3. Pracownik korzysta z oprogramowania w związku z wykonywaniem obowiązków pracowniczych.
4. Pracodawca i Pracownik uzgadniają, że do podstawowych obowiązków Pracownika należy korzystanie z oprogramowania w związku z wykonywaniem obowiązków pracowniczych, zgodne z obowiązującymi przepisami prawa oraz wyłącznie w celach wykonywania obowiązków pracowniczych jak również niekorzystanie z jakiegokolwiek oprogramowania komputerowego, do używania którego Pracodawca nie jest uprawniony w czasie pracy, w miejscu pracy ani przy użyciu sprzętu Pracodawcy.
5. Podpisując porozumienie pracownik jest zobowiązany do przestrzegania zakazu używania pamięci przenośnych (CD, DVD. SD, pamięci USB itp.), bez uzyskania zgody Pracodawcy, Administratora Systemów Informatycznych lub Inspektora Ochrony Danych Osobowych.
6. Pracownik oświadcza, iż jest świadomy odpowiedzialności karnej o której mowa w art. 278 § 2, art. 293, w związku z art. 291 oraz art. 292 ustawy z dnia 6 czerwca 1997 r. kodeks karny (tekst jednolity Dz. U. z 2016 r., poz. 1137) oraz odpowiedzialności karnej i cywilnej przewidzianej w art. 116 i następnych ustawy z dnia 4 lutego 1994 r o prawie autorskim i prawach pokrewnych (tekst jednolity Dz. U. z 2016 r., poz. 666, ze zmianami) za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie oprogramowania.
7. Pracodawca i Pracownik uzgadniają, że naruszenie przez Pracownika jego podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej, może stanowić podstawę do podjęcia przez Pracodawcę przysługujących mu środków prawnych, a w szczególności, może stanowić przyczynę uzasadniającą wypowiedzenie przez Pracodawcę umowy o pracę łączącej Pracodawcę z Pracownikiem lub rozwiązanie przez Pracodawcę tejże umowy o pracę bez wypowiedzenia z winy pracownika, zgodnie z przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jednolity Dz. U. z 2016 r., poz. 1666).
8. Niniejsze porozumienie zostało sporządzone w dwóch egzemplarzach, po jednym dla każdej ze stron.
9. Zmiana, uzupełnienie oraz rozwiązanie niniejszego Porozumienia za zgodą obu stron wymaga formy pisemnej pod rygorem nieważności.
10. Niniejsze porozumienie traci moc z dniem rozwiązania stosunku pracy.

…….……. …….....

/podpis pracownika/ */podpis pracodawcy/*

*- niepotrzebne skreślić