IV.8 *Załącznik nr 8 – Procedura kryzysowa: nieautoryzowany dostęp do systemu Firewall poprzez połączenie sieciowe*

Urząd Gminy Wilkowice	**PROCEDURA JAKOŚCI**					Wersja	Data :
Tytuł	**Procedura kryzysowa : nieautoryzowany dostęp do Systemu Firewall poprzez połączenie sieciowe**						**Strona 1**
1. Cel Procedury	**2. Zakres stosowania**	**3. Opis**	**4. Wymagania**	**5. Wejście**	**6. Wyjście**	**7. Standard**	**PROCES**
Celem niniejszej procedury jest: Określenie metod działania w przypadku powstania sytuacji kryzysowej: nieautoryzowany dostęp do Systemu Firewall poprzez połączenie sieciowe	ABS Systemu Firewall	Procedura ma zapewnić, że kroki podjęte podczas rozwiązywania sytuacji kryzysowej będą optymalne pod względem priorytetów wybranych w Polityce Bezpieczeństwa. Niniejsza procedura dotyczy sytuacji nieautoryzowanego dostępu (lub jej próby) do elementów Systemu Firewall	Istnienie następujących ról w strukturze organizacji: *Główny Administrator Bezpieczeństwa Informacji (GABI) *Administrator Bezpieczeństwa Informacji (ABI) *Administrator Bezpieczeństwa Systemu (ABS) Firewall *Administrator Systemów	Wykrycie nieupoważnionego dostępu (lub prób dostępu) do Systemu Firewall	Wyjaśnienie zaistniałej sytuacji, przywrócenie poprawnej konfiguracji Systemu Firewall	Brak	Poszczególne czynności wykonuje ASB Systemu Firewall 8.1.Sprawdzić aktualnie aktywne połączenia sieciowe na poszczególnych elementach systemu 8.2.Sprawdzić logi poszczególnych elementów Systemu Firewall 8.3.Sprawdzić reguły dostępu do poszczególnych elementów Systemu Firewall 8.4.W przypadku gdy doszło do skanowania Systemu Firewall z Internetu skontaktować się z GABI i ustalić nowe reguły dostępu blokujące dostęp z podejrzanego adresu do Systemu Firewall a także do chronionych przez niego elementów sieci Urzędu Poinformować abusc o zaistniałym incydencie (załącznik 1). Wezwać Administratora Systemów Informatycznych oraz Sekretarza Urzędu 8.5.Sprawdzić stronę producentów poszczególnych elementów systemu, listy

			Informatycznych – Główny Informatyk (ASI)				dyskusyjne i serwisy WWW dotyczące bezpieczeństwa systemów firewall. 8.6.W przypadku gdy zostały odkryte nowe błędy bezpieczeństwa w użytkowanych elementach Systemu Firewall należy sprawdzić czy na stronie domowej producenta nie znajdują się poprawki eliminujące wykryte błędy. Jeżeli są one dostępne należy zainstalować niezbędne poprawki po wcześniejszym kontakcie z GABI 8.7. W przypadku gdy doszło do udanej próby dostępu do poszczególnych elementów Systemu Firewall lub producent stosowanych systemów zabezpieczeń nie dostarczył niezbędnych poprawek należy zwołać Sztab Kryzysowy w którego skład wchodzą: – ABS Systemu Firewall – GABI – ASI – Sekretarz Urzędu 8.8 Spróbować określić w jaki sposób, oraz z jakiego miejsca nastąpił nieuprawniony dostęp do Systemu Firewall. 8.9 Zabezpieczyć logi systemu. 8.10 W przypadku gdy nieuprawniony dostęp nastąpił z Internetu skontaktować się z abuse (załącznik 1) po konsultacji z ASI i za zgodą Wójta 8.11 W przypadku gdy nastąpił nieuprawniony dostęp do Systemu należy zainstalować nową „świeżą" kopię systemu (zarówno systemu operacyjnego jak i oprogramowania firewall) oraz zainstalować wszelkie niezbędne poprawki dostarczane przez producenta lub wezwać jego serwis. 8.12 W przypadku gdy wykryte zostały luki bezpieczeństwa w użytkowanym oprogramowaniu a producent nie dostarczył jeszcze odpowiednich poprawek należy

							wyłączyć System Firewall. System ten musi być włączany wyłącznie na czas konieczny do umożliwienia replikacji danych pomiędzy serwerami i stacjami roboczymi (do replikacji danych należy zestawiać wyłącznie połączenie VPN pomiędzy lokalizacjami urzędu). Przywrócenie Systemu Firewall do normalnego działania powinno nastąpić dopiero po usunięciu wszystkich luk systemowych.
Załączniki	Strona WWW abuse: www.tpnet.pl/abuse.php						
	Adres e – mail : abuse@tpnet.pl						
Lista Kontaktów							
Pieczęć			Podpis			Zatwierdził (Podpis)	

IV.9 *Załącznik nr 9 – Procedura kryzysowa: nieautoryzowany dostęp do serwera przez połączenie sieciowe*

Urząd Gminy Wilkowice	**PROCEDURA JAKOŚCI**					Wersja	Data :
Tytuł	**Procedura kryzysowa : nieautoryzowany dostęp do serwera przez połączenie sieciowe**						**Strona 1**
1. Cel Procedury	**2. Zakres stosowania**	**3. Opis**	**4. Wymagania**	**5. Wejście**	**6. Wyjście**	**7. Standard**	**PROCES**
Celem niniejszej procedury jest: określenie metod działania w przypadku powstania sytuacji kryzysowej: nieautoryzowany dostęp do serwera przez połączenie sieciowe.	Użytkownicy, AS i ABS Systemu	Procedura ma zapewnić, że kroki podjęte podczas rozwiązywania sytuacji kryzysowej będą optymalne pod względem priorytetów wybranych w Polityce Bezpieczeństwa. Niniejsza procedura dotyczy sytuacji, gdy zostaje wykryta próba (udana lub nieudana) nieautoryzowanego dostępu do serwera	Istnienie następujących ról w strukturze organizacji: *Główny Administrator Bezpieczeństwa Informacji (GABI) *Administrator Informacji (AI) *Administrator Bezpieczeństwa Informacji (ABI) *Administrator Bezpieczeństwa Systemu (ABS) *Administrator Systemów Informatycznych – Główny Informatyk (ASI)	Wykrycie próby nieautoryzowanego dostępu do serwera	Przywrócony do poprawnego działania systemu, raport i wyjaśnienie zaistniałej sytuacji.	Brak	Poszczególne czynności wykonuje ABS oraz i ASI 8.1. Sprawdzić aktywne połączenia sieciowe na firewallach oraz na serwerach 1, 2 8.2.Obejrzeć działające procesy na firewallach i serwerach 1,2 8.3.W przypadku podejrzanych połączeń lub procesów należy odłączyć zewnętrzne interfejsy na firewallach 8.4.Sprawdzić jakie pliki były ostatnio wgrywane do serwerów 8.5.Sprawdzić ostatnio uruchamiane polecenia i procesy 8.6.Sprawdzić: *Sprawdzić logi na firewallach *Logi w systemach LINUX *Logi w bazach danych WINDOWS *Logi aplikacji pozostałych 8.7.Jeżeli w wyniku podjętych działań można stwierdzić że: *próba nieuprawnionego dostępu nastąpiła z wnętrza organizacji *w wyniku próby nie nastąpiło naruszenie zasobów na serwerze

							*można określić sprawcę zdarzenia i jego przyczynę to o zaistniałym incydencie należy poinformować ABI i GABI, i zakończyć procedurę. W przeciwnym wypadku należy kontynuować procedurę 8.8.Zwołać Sztab Kryzysowy. W skład Sztabu Kryzysowego wchodzą: *ABS *ABI *GABI 8.9.Jeżeli nadużycie nastąpiło z określonego konta lub stacji roboczej należy zabezpieczyć stację roboczą osoby podejrzanej. 8.10.Skontrolować integralność wszystkich systemów i w razie jej naruszenia odtworzyć na każdym z nich stan z przed zdarzenia z kopii archiwalnych. 8.11.Aby zapewnić możliwość ciągłej pracy systemu w czasie odtwarzania poszczególnych elementów składowych należy przywrócić połączenie sieciowe pomiędzy lokalizacjami urzędu.
Załączniki							
Lista kontaktów	ABS			Imię			Nazwisko
	Stanowisko			Tel:			Tel.kom:
Pieczęć			Podpis				Zatwierdził (podpis)

IV.10 *Załącznik nr 10 – Procedura kryzysowa: wykrycie prób nieautoryzowanego dostępu do komputerów w systemie biurowym Windows*

Urząd Gminy Wilkowice	**PROCEDURA JAKOŚCI**					Wersja	Data :
Tytuł	**Procedura kryzysowa: wykrycie prób nieautoryzowanego dostępu do komputerów w systemie biurowym Windows**						**Strona 1**
1. Cel Procedury	**2. Zakres stosowania**	**3. Opis**	**4. Wymagania**	**5. Wejście**	**6. Wyjście**	**7. Standard**	**PROCES**
Celem niniejszej procedury jest: określenie metod działania w przypadku powstania sytuacji kryzysowej: wykrycie prób nieautoryzowanego dostępu do komputerów w systemie biurowym Windows	Użytkownicy systemu biurowego Windows	Procedura ma zapewnić, że kroki podjęte podczas rozwiązywania sytuacji kryzysowej będą optymalne pod względem priorytetów wybranych w Polityce Bezpieczeństwa. Niniejsza procedura dotyczy sytuacji, gdy zostaje wykryta próba (udana lub nieudana) nieautoryzowanego dostępu do komputerów w systemie biurowym Windows	Istnienie następujących ról w strukturze: *Główny Administrator Bezpieczeństwa Informacji (GABI) *Administrator Bezpieczeństwa Informacji (ABI) *Administrator Bezpieczeństwa Systemu (ABS) *Administrator Systemów Informatycznych – Główny Informatyk (ASI)	Wykrycie w logach systemu biurowego Windows nieautoryzowanego dostępu (lub prób dostępu) do komputerów w systemie biurowym Windows	Raport z zaistniałej sytuacji. Przywrócony do prawidłowego działania system biurowy Windows	Brak	Wszystkie czynności dotyczące systemu biurowego Windows wykonuje ABS. Sprawdzić procesy uruchomione na podejrzanych komputerach 8.1.Sprawdzić aktualnie aktywne połączenia sieciowe na komputerach, do których były próby nieautoryzowanego dostępu (polecenie netstat –a) 8.2.Wyjąć kabel sieciowy z podejrzanych komputerów 8.3.Odłączyć system biurowy Windows od sieci Internet na firewallu Na komputerach dla których doszło do nieuprawnionego dostępu należy sprawdzić: *Uprawnienia do poszczególnych katalogów *Udostępniane zasoby 8.4.Wraz z odpowiednimi sprawdzić: *Sprawdzić logi na firewallach *Sprawdzić logi na komputerach i serwer plików *Sprawdzić konta i grupy dostępne w domenie Windows i na komputerach dla których doszło do nieuprawnionego dostępu oraz zawartość poszczególnych grup użytkowników 8.5.W przypadku gdy próby nieuprawnionego dostępu nastąpiły z danego konta lub stacji należy skontaktować się z osobą, która mogła dokonać tego typu prób. 8.6.Procedura zostaje zakończona w przypadku gdy: *nieuprawniona próba dostępu do systemu biurowego Windows nastąpiła z wnętrza sieci i nie

							zachodzi podejrzenie nieuprawnionego dostępu do danych *sytuacja została wyjaśniona w wyniku rozmowy z osobą z której konta lub stacji dokonano próby nieautoryzowanego dostępu Jeżeli nie zachodzą oba przypadki należy kontynuować procedurę 8.7.Zwołać Sztab Kryzysowy. W skład Sztabu Kryzysowego wchodzą: *ABS *ABI *ASI 8.8.Należy sprawdzić listy dyskusyjne i strony WWW dotyczące bezpieczeństwa systemu Windows oraz zainstalowanego oprogramowania. W przypadku gdy zostały wykryte nowe błędy bezpieczeństwa należy zainstalować niezbędne uaktualnienia na wszystkich komputerach których dany błąd dotyczy 8.9.Jeżeli nadużycie nastąpiło z określonego konta lub stacji roboczej należy wyjąć dyski twarde ze stacji i zainstalować nową kopię systemu na innym dysku 8.10.W przypadku gdy nastąpiło naruszenie danych na serwerze plików należy odtworzyć je z backupu. 8.11.Jeżeli zachodzi podejrzenie, że zostały zmodyfikowane pliki systemowe lub pliki zainstalowanych programów należy zainstalować nową kopię systemu. W przypadku serwera plików oraz komputerów należy odtworzyć niezbędne pliki i dane z backup'u. 8.12.Poinformować o zaistniałym incydencie GABI
Załączniki							
Lista kontaktów	ABS			Imię		Nazwisko	
	Stanowisko			Tel:		Tel.kom:	
Pieczęć			Podpis			Zatwierdził (podpis)	

IV.11 *Załącznik nr 11 – Procedura kryzysowa: nieuprawniona zmiana reguł w systemie Firewall*

Urząd Gminy Wilkowice	**PROCEDURA JAKOŚCI**					Wersja	Data :
Tytuł	**Procedura kryzysowa : nieuprawniona zmiana reguł w Systemie Firewall**						**Strona 1**
1. Cel Procedury	**2. Zakres stosowania**	**3. Opis**	**4. Wymagania**	**5. Wejście**	**6. Wyjście**	**7. Standard**	**PROCES**
Celem niniejszej procedury jest: określenie metod działania w przypadku powstania sytuacji kryzysowej: nieuprawniona zmiana reguł w Systemie Firewall	ABS	Procedura ma zapewnić, że kroki podjęte podczas rozwiązywania sytuacji kryzysowej będą optymalne pod względem priorytetów wybranych w Polityce Bezpieczeństwa. Niniejsza procedura dotyczy sytuacji, gdy zostaje wykryta zmiana reguł dostępu w Systemie Firewall	Istnienie następujących ról w strukturze organizacji: *Główny Administrator Bezpieczeństwa Informacji (GABI) *Administrator Bezpieczeństwa Informacji (ABI) *Administrator Bezpieczeństwa Systemu (ABS)	Wykrycie zmiany reguł dostępu w Systemie Firewall	Przywrócone poprawne reguły dostępu w Systemie Firewall. Wyjaśnienie przyczyny incydentu.	Brak	Poszczególne czynności wykonuje ABS 8.1.Porównnać aktualne reguły dostępu w Systemie Firewall z regułami dostępu wyspecyfikowanymi w załączniku 19 do Polityki Bezpieczeństwa 8.2.Sprawdzić logi Systemu Firewall 8.3.Ustalić przyczynę zmiany reguł 8.4.Jeżeli zachodzi podejrzenie, że zmiana reguł jest wynikiem nieuprawnionego dostępu do systemu należy rozpocząć procedurę kryzysową „nieautoryzowany dostęp do Systemu Firewall poprzez połączenie sieciowe". 8.5.Jeżeli nie zachodzi sytuacja z punktu 8.4 należy przywrócić prawidłowe reguły dostępu po uprzednim kontakcie z GABI
Załączniki							

Lista kontaktów			
Pieczęć		Podpis	Zatwierdził (podpis)

IV.12 *Załącznik nr 12 – Procedura kryzysowa: działanie obcego oprogramowania na komputerze – stacji roboczej*

Urząd Gminy Wilkowice	**PROCEDURA JAKOŚCI**				Wersja	Data :
Tytuł	**Procedura kryzysowa : działanie obcego oprogramowania na komputerze – stacji roboczej**					**Strona 1**
1. Cel Procedury	**2. Zakres stosowania**	**3. Opis**	**4. Wymagania**	**5. Wejście**	**6. Wyjście**	**7. Standard**	**PROCES**
Celem niniejszej procedury jest: określenie metod działania w przypadku powstania sytuacji kryzysowej: działanie obcego oprogramowania na komputerze – stacji roboczej (K-ST).	Użytkownicy, Administrator Bezpieczeństwa Systemu i Administrator Systemu Biurowego Windows	Procedura ma zapewnić, że kroki podjęte podczas rozwiązywania sytuacji kryzysowej będą optymalne pod względem priorytetów wybranych w Polityce Bezpieczeństwa. Niniejsza procedura dotyczy sytuacji, gdy zostaje wykryte działanie obcego oprogramowania na komputerze (K-ST)	Istnienie następujących ról w strukturze organizacji: *Główny Administrator Bezpieczeństwa Informacji (GABI) *Administrator Bezpieczeństwa Informacji (ABI) *Administrator Bezpieczeństwa Systemu (ABS) *Administrator Systemów Informatycznych – Główny Informatyk (ASI)	Wykrycie działania obcego oprogramowania na komputerze (K-ST)	Przywrócony do poprawnego działania system na K-ST i raport z zaistniałej sytuacji.	Brak	Poszczególne czynności wykonuje ABS lub ASI 8.1.Sprawdzić aktualnie aktywne połączenia sieciowe (polecenie netstat –a). 8.2.Wyjąć kabel sieciowy z komputera 8.3.Sprawdzić logi systemowe komputera 8.4.Sprawdzić logi systemowe aplikacji 8.5.Sprawdzić uruchomione na komputerze procesy. 8.6.Sprawdzić rejestry systemowe na komputerze (załącznik 1) 8.7.Sprawdzić jakie pliki były ostatnio kasowane. 8.8..Sprawdzić jakie pliki były ostatnio wgrywane na komputer 8.9.Spróbować określić sposób działania niepożądanego programu 8.10.Sprawdzić logi na firewall. 8.11.W przypadku gdy w wyniku przeprowadzonych czynności można jednoznacznie stwierdzić, że: – obcy proces nie jest procesem niebezpiecznym – można ustalić osobę odpowiedzialną za uruchomienie procesu

							należy: – „zabić" proces – usunąć jego pliki z dysku twardego – poinformować o incydencie ABI – zakończyć procedurę. W innym przypadku należy kontynuować procedurę. 8.12.Zwołać Sztab Kryzysowy. W skład Sztabu Kryzysowego wchodzą: – ABS – ABI – ASI 8.13.„zabić" obcy proces 8.14.Spróbować znaleźć drogę, jaką obce oprogramowanie mogło dostać się na komputer HOME 8.15.W przypadku gdy zostały naruszone pliki systemowe zainstalować system i aplikację z oryginalnych nośników 8.16.W przypadku gdy zostały naruszone pliki aplikacji zainstalować aplikację z oryginalnych nośników, w innym przypadku usunąć niepożądane oprogramowanie 8.17.Zmienić hasła dostępowe do systemu Windows i aplikacji 8.18.Poinformować GABI o zaistniałym incydencie
Załączniki							
Lista Kontaktów	ABS Systemu Firewall			Imię			Nazwisko
	Stanowisko			Tel:			Tel.kom:
Pieczęć			Podpis				Zatwierdził (Podpis)

IV.13 *Załącznik nr 13 – Procedura kryzysowa: obcy proces działający na serwerze*

Urząd Gminy Wilkowice	**PROCEDURA JAKOŚCI**					Wersja	Data :
Tytuł	**Procedura kryzysowa : obcy proces działający na serwerze**						**Strona 1**
1. Cel Procedury	**2. Zakres stosowania**	**3. Opis**	**4. Wymagania**	**5. Wejście**	**6. Wyjście**	**7. Standard**	**PROCES**
Celem niniejszej procedury jest: określenie metod działania w przypadku powstania sytuacji kryzysowej: obcy proces działający na serwerze	Użytkownicy, ABS,ASI	Procedura ma zapewnić, że kroki podjęte podczas rozwiązywania sytuacji kryzysowej będą optymalne pod względem priorytetów wybranych w Polityce Bezpieczeństwa. Niniejsza procedura dotyczy sytuacji, gdy zostaje wykryty obcy proces działający na serwerze	Istnienie następujących ról w strukturze *Administrator Bezpieczeństwa Informacji (ABI) *Główny Administrator Bezpieczeństwa Informacji (GABI) *Administrator Systemów Informatycznych (ASI) *Administrator Bezpieczeństwa Systemu (ABS)	Wykrycie działania obcego procesu działającego na serwerze	Przywrócony do poprawnego działania System Serwer raport z zaistniałej sytuacji.	Brak	Poszczególne czynności wykonuje ABS i ASI 8.1.Sprawdzić aktualnie aktywne połączenia sieciowe 8.2.Wyjąć kabel sieciowy z serwera jeśli pojawiłyby się jakieś podejrzane połączenia (pokazane przez netstat). 8.3.Obejrzeć podejrzany proces – Kto uruchomił – Jak długo działa – Spróbować dojść co proces robi 8.4.Sprawdzić jakie pliki były ostatnio wgrywane na serwery 1, 2 8.5.Sprawdzić: – Sprawdzić logi na firewallach – Logi w systemach Linux – Logi w bazie danych Windows – Logi aplikacji pozostałych 8.6.Obejrzeć historię poleceń 8.7.Jeżeli w wyniku podjętych działań nie można jednoznacznie wykluczyć, że działający proces nie jest obcym, potencjalnie niebezpiecznym procesem –

							kontynuować procedurę. W przeciwnym wypadku koniec procedury 8.8.„Zabić" proces. 8.9.Zwołać Sztab Kryzysowy. W skład Sztabu Kryzysowego wchodzą: – ABS – ABI – GABI – ASI 8.10.Skontrolować integralność systemu plików wszystkich systemów.W momencie stwierdzenia naruszenia odtworzyć z kopii archiwalnych stan wszystkich systemów z przed zdarzenia. Odtwarzanie systemu Serwer należy przeprowadzić zgodnie z wytycznymi z punktu 8.12 Procedury kryzysowej: „Nieautoryzowany dostęp do serwera poprzez połączenie sieciowe". 8.11.W czasie odtwarzania stanu poszczególnych systemów należy monitorować procesy i połączenia na dostępnych serwerach.
Załączniki							
Lista Kontaktów	ABS			Imię		Nazwisko	
	Stanowisko			Tel:		Tel.kom:	
Pieczęć			Podpis			Zatwierdził (Podpis)	

IV.14 *Załącznik nr 14 – Procedura kryzysowa: utrata połączenia VPN między lokalizacjami urzędu*

Urząd Gminy Wilkowice	**PROCEDURA JAKOŚCI**					Wersja	Data :
Tytuł	**Procedura kryzysowa : utrata połączenia VPN między lokalizacjami Urzędu**						**Strona 1**
1. Cel Procedury	**2. Zakres stosowania**	**3. Opis**	**4. Wymagania**	**5. Wejście**	**6. Wyjście**	**7. Standard**	**PROCES**
Celem niniejszej procedury jest: określenie metod działania w przypadku powstania sytuacji kryzysowej: utrata połączenia VPN między lokalizacjami urzędu.	ABS i ASI	Procedura ma zapewnić, że kroki podjęte podczas rozwiązywania sytuacji kryzysowej będą optymalne pod względem priorytetów wybranych w Polityce Bezpieczeństwa. Niniejsza procedura dotyczy sytuacji, gdy zostaje wykryta utrata połączenia VPN pomiędzy lokalizacjami Urzędu	Istnienie następujących ról w strukturze organizacji: *Główny Administrator Bezpieczeństwa Informacji (GABI) *Administrator Bezpieczeństwa Informacji (ABI) *Administrator Bezpieczeństwa Systemu (ABS) *Administrator Systemów Informatycznych (ASI)	Utrata połączenia VPN pomiędzy Lokalizacjami Urzędu	Przywrócone połączenie VPN. Raport i wyjaśnienie zaistniałej sytuacji	Brak	Poszczególne czynności wykonuje ABS i ASI 8.1.Sprawdzić logi systemu firewall 8.2.Sprawdzić połączenie z siecią Internet 8.3.W przypadku gdy nie ma połączenia z Internetem skontaktować się z dostawca Internetu. 8.4.Sprawdzić listy dyskusyjne i strony WWW dotyczące bezpieczeństwa używanych elementów Systemu Firewall 8.5.Jeżeli utrata połączenia jest wynikiem braku działania lub błędu w Systemie Firewall zainstalować niezbędne patche udostępniane przez producenta. 8.6.W przypadku podejrzenia, że utrata połączenia jest wynikiem nieuprawnionego dostępu do Systemu Firewall rozpocząć procedurę kryzysową „nieautoryzowany dostęp do Systemu Firewall poprzez połączenie sieciowe" 8.7.Przywrócić połączenie VPN pomiędzy lokalizacjami urzędu 8.8.O zaistniałym incydencie poinformować GABI

Załączniki	Nr telefonu do pomocy technicznej dostawcy Internet		
	Nr telefonu do dostawcy systemu Firewall		
Lista Kontaktów			
Pieczęć	Podpis	Zatwierdził (Podpis)	

IV.15 *Załącznik nr 15 – Procedura kryzysowa: utrata danych z serwera*

Urząd Gminy Wilkowice	**PROCEDURA JAKOŚCI**					Wersja	Data :
Tytuł	**Procedura kryzysowa : utrata danych z serwera**						**Strona 1**
1. Cel Procedury	**2. Zakres stosowania**	**3. Opis**	**4. Wymagania**	**5. Wejście**	**6. Wyjście**	**7. Standard**	**PROCES**
Celem niniejszej procedury jest: określenie metod działania w przypadku powstania sytuacji kryzysowej: utrata danych z serwerów.	Użytkownicy, ABS, ASI, Sekretarz Urzędu	Procedura ma zapewnić, że kroki podjęte podczas rozwiązywania sytuacji kryzysowej będą optymalne pod względem priorytetów wybranych w Polityce Bezpieczeństwa. Niniejsza procedura dotyczy sytuacji, gdy nastąpi utrata danych z serwera	Istnienie następujących ról w strukturze organizacji: *Główny Administrator Bezpieczeństwa Informacji (GABI) *Administrator Systemów Informatycznych (ASI) *Administrator Bezpieczeństwa Informacji (ABI) *Administrator Bezpieczeństwa Systemu (ABS)	Utrata danych z serwera	Przywrócony do poprawnego działania System Serwer, raport z zaistniałej sytuacji	Brak	Poszczególne czynności wykonuje ABS i ASI 8.1.Sprawdzić aktualnie aktywne połączenia sieciowe 8.2.W przypadku stwierdzenia podejrzanych połączeń wyjąć kabel sieciowy z serwera na którym stwierdzono utratę danych. 8.3.Sprawdzić: *Sprawdzić logi na firewallach *Logi w systemach LINUX *Logi bazy danych WINDOWS *Logi aplikacji pozostałych *Jeżeli w wyniku podjętych działań można jednoznacznie stwierdzić, że utrata danych nie jest wynikiem celowego i nieuprawnionego działania należy odtworzyć dane z backup'u, w przeciwnym razie należy przejść do punktu 8.5 *W przypadku utraty danych z serwera należy odtworzyć dane wyłącznie na tym serwerze a następnie wymusić replikację danych i należy poinformować użytkowników systemu o zaistniałej sytuacji. O zaistniałej sytuacji należy poinformować ABI, GABI, Sekretarza Urzędu 8.4.Zwołać Sztab Kryzysowy. W skład Sztabu Kryzysowego wchodzą: – ABS

							– ABI – GABI – ASI 8.5.Skontrolować integralność systemu na którym stwierdzono utratę danych, a także integralność pozostałych systemów wchodzących w skład systemu. W przypadku gdy zachodzi podejrzenie, że zaistniała sytuacja jest wynikiem nieautoryzowanego dostępu do serwera należy odtworzyć z kopii archiwalnych stan wszystkich systemów z przed zdarzenia. Odtwarzanie systemu Serwer Klientów należy przeprowadzić zgodnie z wytycznymi z punktu 8.12 Procedury kryzysowej: „Nieautoryzowany dostęp do serwera 1przez połączenie sieciowe".
Załączniki							
Lista Kontaktów	ABS			Imię			Nazwisko
	Stanowisko			tel:			Tel.kom:
Pieczęć			Podpis				Zatwierdził (Podpis)

IV.16 *Załącznik nr 16 – Procedura kryzysowa: wykrycie wirusa w systemie biurowym Windows*

Urząd Gminy Wilkowice	**PROCEDURA JAKOŚCI**					Wersja	Data :
Tytuł	**Procedura kryzysowa: wykrycie wirusa w systemie biurowym Windows**						**Strona 1**
1. Cel Procedury	**2. Zakres stosowania**	**3. Opis**	**4. Wymagania**	**5. Wejście**	**6. Wyjście**	**7. Standard**	**PROCES**
Celem niniejszej procedury jest: określenie metod działania w przypadku powstania sytuacji kryzysowej: wykrycie wirusa w systemie biurowym Windows	Użytkownicy systemu biurowego Windows, ASI i ABS	Procedura ma zapewnić, że kroki podjęte podczas rozwiązywania sytuacji kryzysowej będą optymalne pod względem priorytetów wybranych w Polityce Bezpieczeństwa. Niniejsza procedura dotyczy sytuacji, gdy zostaje wykryty wirus systemie biurowym Windows	Istnienie następujących ról w strukturze: *Główny Administrator Bezpieczeństwa Informacji (GABI) *Administrator Bezpieczeństwa Informacji (ABI) *Administrator Bezpieczeństwa Systemu (ABS) *Administrator Systemów Informatycznych (ASI)	Wykrycie wirusa w systemie biurowym Windows	Usunięty wirus z systemu biurowego Windows. Raport z zaistniałej sytuacji	Brak	Wszystkie czynności wykonuje ABS i ASI 8.1.Określić przyczyny podejrzanego zachowania się aplikacji i systemów wchodzących w skład systemu biurowego Windows. W przypadku gdy zachodzi podejrzenie działania wirusa postępować według następnych punktów w przeciwnym razie koniec procedury. 8.2.Sprawdzić stronę WWW producenta zainstalowanego oprogramowania antywirusowego pod kątem dostępnych uaktualnień do posiadanej bazy wirusów. Jeżeli jest dostępne rozszerzenie posiadanej bazy wirusów należy ją uaktualnić 8.3.Sprawdzić strony WWW innych producentów oprogramowania antywirusowego 8.4.Sprawdzić podejrzaną stację roboczą lub serwer przy pomocy posiadanego oprogramowania antywirusowego 8.5.Sprawdzić pozostałe komputery w systemie biurowym Windows 8.6.W przypadku wykrycia wirusa należy go usunąć. 8.7.W przypadku gdy zachodzi podejrzenie, że zaistniały incydent jest wynikiem naruszenia Polityki Bezpieczeństwa firmy zwołać Sztab Kryzysowy. W skład Sztabu Kryzysowego

							wchodzą: – ABS – ABI – ASI 8.8.Określić sposób zainfekowania oprogramowania w systemie biurowym Windows 8.9.W przypadku stwierdzenia naruszenia polityki bezpieczeństwa wyciągnąć. konsekwencje służbowe w stosunku do osoby odpowiedzialnej za jego zaistnienie. 8.10.Poinformować o zaistniałym incydencie GABI
Załączniki							
Lista Kontaktów							

Pieczęć	Podpis	Zatwierdził (Podpis)

IV.17 *Załącznik nr 17 – Procedura kryzysowa: możliwość połączenia typu dial-in do komputera – stacji roboczej*

Urząd Gminy Wilkowice	**PROCEDURA JAKOŚCI**					Wersja	Data :
Tytuł	**Procedura kryzysowa : możliwość połączenia typu dial – in do komputera – stacji roboczej**						**Strona 1**
1. Cel Procedury	**2. Zakres stosowania**	**3. Opis**	**4. Wymagania**	**5. Wejście**	**6. Wyjście**	**7. Standard**	**PROCES**
Celem niniejszej procedury jest: określenie metod działania w przypadku powstania sytuacji kryzysowej: możliwość połączenia typu dial – in do komputera – stacji roboczej (K-ST)	Użytkownicy ABS, ASI	Procedura ma zapewnić, że kroki podjęte podczas rozwiązywania sytuacji kryzysowej będą optymalne pod względem priorytetów wybranych w Polityce Bezpieczeństwa. Niniejsza procedura dotyczy sytuacji, gdy zostaje wykryta zmiana w konfiguracji komputera umożliwiająca połączenie typu	Istnienie następujących ról w strukturze organizacji: *Główny Administrator Bezpieczeństwa Informacji (GABI) *Administrator Systemów Informatycznych (ASI) *Administrator Bezpieczeństwa Informacji (ABI) *Administrator Bezpieczeństwa Systemu (ABS)	Wykrycie zmiany konfiguracj i modemu komputera	Raport z zaistniałej sytuacji. Wyjaśnienie przyczyn incydentu. Przywrócon a poprawna konfiguracja systemu	Brak	Poszczególne czynności wykonuje ABS i ASI 8.1.Sprawdzić konfigurację oprogramowania modemu na komputerze 8.2.W przypadku gdy nie stwierdzono zmiany konfiguracji – koniec procedury w przeciwnym razie należy kontynuować procedurę 8.3.Sprawdzić logi systemowe na komputerze 8.4.Sprawdzić logi Systemu Firewall 8.5.Sprawdzić uprawnienia do poszczególnych plików i katalogów w systemie Windows 8.6.Sprawdzić jakie pliki były ostatnio kasowane i wgrywane na komputerze 8.7.Sprawdzić bazę użytkowników stacji oraz zawartość poszczególnych grup użytkowników 8.8.Zwołać Sztab Kryzysowy. W skład Sztabu Kryzysowego wchodzą: – ABS – ABI – ASI 8.9.Określić przyczynę i sprawcę incydentu 8.10.Przywrócić poprawną konfigurację systemu

		dial – in.					8.11.Jeżeli stwierdzono, że zostały zmienione pliki systemowe – zainstalować system i aplikację z oryginalnych nośników. 8.12.Jeżeli stwierdzono, że zostały zmienione pliki aplikacji – zainstalować aplikację z oryginalnych nośników. 8.13.Zmienić hasła dostępowe do systemu Windows i aplikacji stacji roboczej 8.14.Poinformować GABI o zaistniałym incydencie
Załączniki							
Lista Kontaktów	ABS			Imię			Nazwisko
	Stanowisko			Tel:			Tel.kom:
Pieczęć			Podpis				Zatwierdził (Podpis)

IV.18 *Załącznik nr 18 - Instrukcja BHP przy obsłudze stanowiska komputerowego*

UWAGI OGÓLNE

1. Do pracy przy obsłudze komputera może być skierowany pracownik, który posiada:
   - wymagane odpowiednimi przepisami kwalifikacje do pracy na wyznaczonym stanowisku;
   - odpowiedni stan zdrowia, potwierdzony świadectwem lekarskim.
2. Do pracy należy przystępować w stanie trzeźwości, zachowując schludny i estetyczny wygląd.
3. Należy zapewnić bezpieczne warunki pracy przy obsłudze komputera poprzez:
   - zapewnienie wystarczającej powierzchni stanowiska pracy;
   - dostateczną wentylację naturalną lub mechaniczną pomieszczenia;
   - zapewnienie wystarczającego komfortu cieplnego w okresie jesienno zimowym.

PODSTAWOWE CZYNNOŚCI PRZED ROZPOCZĘCIEM PRACY

PRACOWNIK POWINIEN:
1. Wywietrzyć pomieszczenie.
2. Skontrolować wyposażenie stanowiska.
3. Dostosować biurko, krzesło i podnóżek do wymiarów swojego ciała.
4. Przygotować komputer do pracy poprzez:
   - podłączenie do sieci zasilającej;
   - wyświetlenie na ekranie dowolnej informacji z uruchomionego programu;
   - regulację jasności i kontrastu pomiędzy znakami i tłem w zależności od potrzeb i aktualnych warunków otoczenia;
   - zastosowanie filtra lub ekranu ochronnego.
5. Przygotować potrzebne dokumenty oraz programy użytkowe do pracy.

CZYNNOŚCI WYKONYWANE PODCZAS PRACY

PRACOWNIK POWINIEN:
1. Zapewnić przed klawiaturą wystarczającą przestrzeń na podparcie rąk i dłoni.
2. Stosować odległość ekranu monitora od oczu wynoszącą od 1,5 do 2 przekątnych ekranu.
3. Nie dopuścić do dostępu do komputera osób nie upoważnionych.
4. Zgłaszać przełożonemu wszelkie nieprawidłowości oraz niesprawności sprzętu.

CZYNNOŚCI ZABRONIONE

PRACOWNIKOWI ZABRANIA SIĘ:
1. Spożywania posiłków podczas pracy.
2. Palenia tytoniu w pomieszczeniach pracy z komputerem.
3. Samowolnego naprawiania urządzeń komputerowych, sprzętu i wyposażenia zasilanego energią elektryczną.
4. Uszkadzania /zrywania/ plomb zabezpieczających sprzęt komputerowy.
5. Przechowywania na stanowisku pracy magnesów i metali namagnesowanych tudzież noszenia biżuterii magnetycznej podczas pracy.

CZYNNOŚCI PO ZAKOŃCZENIU PRACY

PRACOWNIK POWINIEN:

1. Wyłączyć komputer, monitor, drukarkę i pozostałe urządzenia oraz sprzęt stanowiskowy zasilany energią elektryczną.
2. Uporządkować i sprzątnąć stanowisko pracy.
3. Pozamykać szafy i biurko.
4. Kopie bezpieczeństwa, dyskietki oraz wyjmowane dyski twarde zamknąć w sejfie.
5. Wytrzeć kurz miękką szmatką z powierzchni blatów, biurka, urządzeń i sprzętu.
6. Zabezpieczyć urządzenia przed dostępem osób niepowołanych.

UWAGI KOŃCOWE

1. Kobiety w ciąży nie mogą pracować bezpośrednio przy monitorze ekranowym.
2. W czasie intensywnej pracy przy obsłudze monitora należy stosować przerwy (10 minut po godzinie pracy lub 20 minut po 2 godzinach pracy).
3. W razie wątpliwości, co do zachowania warunków bezpieczeństwa pracy przy wykonywaniu poleconych czynności, pracownik ma prawo przerwać pracę i zwrócić się do przełożonego o wyjaśnienie zaistniałej sytuacji.

ZATWIERDZAM

Data i podpis pracodawcy