PW_3.6.5-2/Z4

WYTYCZNE DLA DOSTAWCÓW PRZETWARZAJĄCYCH DOKUMENTACJĘ NCBR (CENTRUM) W FORMIE ELEKTRONICZNEJ

1. Dostawca zobowiązany jest do ochrony poufności, integralności i dostępności dokumentacji elektronicznej przekazanej im przez Centrum.
2. Dostawca zobowiązany jest do kontrolowania dostępu do dokumentacji Centrum w formie elektronicznej. W szczególności dostęp do przedmiotowej dokumentacji posiadają wyłącznie osoby wykonująca zadania, do których niezbędny jest dostęp do przedmiotowej dokumentacji. W przypadku ustania takiej potrzeby dostęp do dokumentacji jest odbierany.
3. Dopuszcza się wykonywanie kopii dokumentacji w przypadku, gdy jest to zasadne optymalizacją organizacji pracy. Kopia dokumentacji podlega identycznym zasadom bezpieczeństwa, jak w przypadku dokumentacji oryginalnej udostępnionej przez Centrum.
4. Dopuszcza się wykonywanie papierowych kopii dokumentacji Centrum poprzez ich wydruk. W takim przypadku dostawca stosuje, w zakresie ochrony dokumentacji papierowej, właściwe zasady bezpieczeństwa określone przez Centrum.
5. Dostawca jest zobowiązany do trwałego usunięcia przekazanej mu przez Centrum dokumentacji oraz wszystkich sporządzonych kopii tej dokumentacji, w przypadku:
   1) zakończenia świadczenia usług na rzecz Centrum;
   2) ustania potrzeby przetwarzania dokumentacji przez dostawcę;
   3) na każde żądanie Centrum.
6. Dostawca jest zobowiązany, na żądanie Centrum, do pisemnego potwierdzenia faktu usunięcia dokumentacji i wszystkich jej kopii zgodnie z ustępem powyżej. Powyższy ustęp dotyczy również dokumentacji przechowywanej w postaci kopii zapasowych.
7. Dostawca jest zobowiązany do przetwarzania dokumentacji Centrum na sprzęcie informatycznym spełniającym poniżej wyszczególnione minimalne wymagania bezpieczeństwa:
   1) sprzęt informatyczny posiada mechanizm kontroli dostępu do danych zapewniających ochronę przed dostępem osób nieuprawnionych do przetwarzanych w nim informacji.
   2) system operacyjny posiada zainstalowane wszystkie dostępne aktualizacje zabezpieczeń;
   3) w systemie operacyjnym zainstalowany jest system antywirusowy, a jego sygnatury są aktualne;
   4) w systemie operacyjnym firewall jest uruchomiony i posiada konfigurację uniemożliwiającą inicjowanie połączeń przychodzących oraz umożliwiającą nawiązywanie połączeń wychodzących tylko przez zatwierdzone procesy;
   5) zainstalowane na komputerze oprogramowanie pochodzi z zaufanych źródeł;

8. Dostawca może umożliwić dostęp do dokumentacji Centrum wyłącznie osobom posiadającym wiedzę z zakresu bezpiecznej eksploatacji systemów informatycznych i ochrony przed cyberzagrożeniami, w tym atakami phishingowymi. Dostawca jest zobowiązany do poinformowania osób wskazanych powyżej o obowiązku zabezpieczenia dokumentacji Centrum przed dostępem do niej osób nieuprawnionych.
9. Zabroniona jest praca nad dokumentacją Centrum w miejscach publicznych, za wyjątkiem sytuacji, gdy w związku z zadaniami realizowanymi w związku ze współpracą z Centrum dostawca dokonuje prezentacji dokumentów sklasyfikowanych jako K1.
10. Praca z dokumentami oznaczonymi K3 lub K2 odbywa się wyłącznie w pomieszczeniach do których dostęp mają wyłącznie upoważnione osoby.
11. Dokumenty sklasyfikowane jako K3 i K2 mogą być co do zasady przechowywane na sprzęcie stacjonarnym, znajdującym się w pomieszczeniach dostawcy zabezpieczonych przed dostępem osób nieupoważnionych. Dopuszcza się przechowywanie dokumentów sklasyfikowanych K3 i K2 na komputerach przenośnych wyłącznie w przypadku zastosowania szyfrowania, przy czym wymagane jest zastosowanie szyfrowania z wykorzystaniem algorytmu AES-256 lub mocniejszego.
12. Zabrania się przechowywania dokumentów sklasyfikowanych jako K3 na nośnikach przenośnych. Dokumenty sklasyfikowane jako K2 mogą być przechowywane na nośnikach przenośnych wyłącznie w postaci szyfrowanej, przy czym wymagane jest szyfrowanie z wykorzystaniem algorytmu AES-256 lub mocniejszego.
13. W przypadku przesyłania dokumentów sklasyfikowanych jako K3 i K2 w sposób stwarzający ryzyko dostępu do nich przez osoby nieuprawnione, w szczególności przy przesyłaniu dokumentów za pośrednictwem Internetu, wymagane jest stosowanie ochrony kryptograficznej z wykorzystaniem algorytmu AES-256 lub mocniejszego.
14. Dopuszcza się szyfrowanie dokumentów z wykorzystaniem haseł, o ile spełnione są wymagania dotyczące algorytmu kryptograficznego, zaś siła hasła odpowiada kluczowi o długości 256 bitów.
15. Każde podejrzenie naruszenia bezpieczeństwa dokumentacji przekazanej przez Centrum należy każdorazowo zgłaszać opiekunowi dostawcy oraz na adres: incydent@ncbr.gov.pl.
16. Dostawca jest zobowiązany, na wniosek Centrum, do złożenia niezbędnych wyjaśnień w związku z podejrzeniem naruszenia bezpieczeństwa.