JAK ZORGANIZOWAĆ PRACĘ ZDALNĄ W FIRMIE – CHECKLISTA DLA DZIAŁÓW IT

CO POWINIENEM ZROBIĆ?
Przypomnij pracownikom obowiązujące w firmie **procedury odnoszące się do pracy zdalnej.**
Wydaj pracownikom sprzęt, na którym mają pracować (m.in. laptopy, telefony komórkowe), pamiętając w szczególności o: 1) zaszyfrowaniu dysków, kart pamięci lub innych elektronicznych nośników informacji, 2) przyznaniu pracownikom adekwatnych do ich roli w organizacji praw dostępu (domyślnie jako użytkownicy), 3) potwierdzeniu, że został zainstalowany system antywirusowy, 4) włączeniu wszystkich funkcji bezpieczeństwa (np. hasła, automatyczne blokady ekranu, zdalne usuwanie zawartości sprzętu), 5) włączeniu wszystkich automatycznych aktualizacji dla systemu operacyjnego, aplikacji oraz systemu antywirusowego.
Przekaż pracownikom informacje, w jaki sposób mogą kontaktować się z Tobą w przypadku problemów technicznych (podaj adres e-mail lub/i numer telefonu).
Poproś pracowników, aby zobowiązali się do korzystania z Internetu służbowego (np. hotspot Wifi z telefonu służbowego), a jeżeli nie jest to możliwe poproś ich o potwierdzenie, że zmienili domyślne hasło do domowego routera, i że odpowiada ono zasadom bezpieczeństwa ustanowionym w Twojej organizacji.
Zobowiąż pracowników, aby przed zalogowaniem się do systemów firmowych połączyli się z VPN.
Poproś pracowników, aby przeznaczyli wybraną część swojego mieszkania do wykonywania pracy zdalnej oraz ograniczyli dostęp do niej osobom postronnym (członkowie rodziny, znajomi, dostawcy żywności).
Zobowiąż pracowników do ochrony drukowanych przez nich dokumentów przed nieautoryzowanym dostępem osób postronnych.
Zobowiąż pracowników do przechowywania wszystkich wytworzonych informacji na firmowych serwerach. Jeśli nie jest to możliwe, czasowe przechowywanie informacji firmowych na urządzeniach mobilnych chronionych hasłem i zaszyfrowanych (np. laptopie, dysku przenośnym) jest dozwolone za uprzednią zgodą działu IT.
Przygotuj i przeszkól pracowników na zagrożenia związane z pracą zdalną (np. phishing, malware, USB killer).
Monitoruj ruch sieciowy pod kątem możliwych anomalii.
Przeskanuj urządzenia pracowników pod kątem szkodliwego oprogramowania przed ponownym podłączeniem ich do sieci służbowej. Niezależnie od powyższego możesz wykonać ponowną instalację systemu operacyjnego, co będzie dobrym pretekstem do usunięcia niepotrzebnych plików i przeniesienia plików zapisanych dotychczas lokalnie na Twój serwer firmowy.
Wskaż z kim pracownicy powinni się kontaktować w przypadku incydentów związanych z bezpieczeństwem informacji.