Załącznik nr 1 do Procedury zdalnego kształcenia uczniów Szkoły Podstawowej im. Zjednoczonej Europy w Starkowie

ZASADY KORZYSTANIA Z URZĄDZEŃ PRYWATNYCH DO CELÓW SŁUŻBOWYCH POZA OBSZAREM ADMINISTRATORA DANYCH OSOBOWYCH

§ 1.

1. Niniejsza zasady dotyczą pracowników Szkoły Podstawowej im. Zjednoczonej Europy w Starkowie, którzy w ramach wykonywania obowiązków służbowych przetwarzają dane osobowe za pośrednictwem urządzeń mobilnych (tj. laptop, tablet, notebook, smartfon, telefon komórkowy) poza obszarem Administratora Danych Osobowych.
2. Ilekroć w jest mowa o:
   1) **Administratorze Danych Osobowych** - należy przez to rozumieć Szkołę Podstawową im. Zjednoczonej Europy w Starkowie reprezentowaną przez Dyrektora jednostki;
   2) **Urządzeniu mobilnym** – należy przez to rozumieć (przenośne) urządzenie elektroniczne pozwalające na przetwarzanie, odbieranie oraz wysyłanie danych bez konieczności utrzymywania przewodowego połączenia z siecią;
   3) **Użytkowniku systemu** – należy przez to rozumieć osobę przetwarzającą dane osobowe za pośrednictwem systemu informatycznego, posiadającą upoważnienie wydane przez Administratora Danych Osobowych lub osobę przez niego uprawnioną dopuszczoną do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu;
   4) **Systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zastosowanych w celu przetwarzania danych osobowych.
3. Każda osoba przetwarzająca dane osobowe za pośrednictwem urządzeń mobilnych poza obszarem Administratora Danych Osobowych zobowiązana jest do stosowania niniejszych zasad.

§ 2.

1. Stacja robocza (komputer stacjonarny, notebook, netbook) wykorzystywana do przetwarzania danych osobowych musi spełniać następujące wymagania:
   1) system operacyjny musi być legalny oraz musi być na nim aktywna funkcja automatycznej aktualizacji;
   2) wszelkie oprogramowanie wykorzystywane w trakcie pracy musi być legalne, a jego licencja musi umożliwiać wykorzystywanie w innych celach niż osobiste;
   3) oprogramowanie antywirusowe musi być stale włączone z aktywną funkcją automatycznej aktualizacji;

4) oprogramowanie służące ochronie przed zagrożeniami płynącymi z sieci publicznej (zapora ogniowa) musi być stale włączone z aktywną funkcją automatycznej aktualizacji;
5) system operacyjny musi zostać wyposażony w konto użytkownika wykorzystywane wyłącznie przez użytkownika systemu. Hasło do konta użytkownika musi pozostać poufne i może być wykorzystywane wyłącznie przez użytkownika systemu informatycznego;
6) system operacyjny musi być wyposażony w funkcję automatycznego wygaszenia ekranu, po którego aktywacji wznowienie będzie wymagało podania hasła do konta użytkownika.

2. Jeżeli w ramach przetwarzania danych osobowych korzystając z prywatnych urządzeń informatycznych następuje komunikacja za pośrednictwem sieci publicznej (wchodzenie na strony internetowe, wysyłanie i odbieranie wiadomości elektronicznych, wykorzystywanie oprogramowania służącego wymianie informacji w sieci publicznej) dostęp do sieci musi być zabezpieczony poprzez zastosowanie hasła dostępu.

§ 3.

1. Użytkownicy zobowiązani są do:
   1) korzystania z urządzeń w sposób uniemożliwiający osobom nieupoważnionym wgląd w wykonywaną pracę (zabezpieczenie dostępu do urządzenia hasłem, szyfrowanie plików, zabezpieczenie środkami ochrony kryptograficznej, urządzenia powinny być zaopatrzone w minimalne dane kontaktowe właściciela);
   2) zabezpieczania dostępu do sprzętu służbowego oraz posiadanych danych i informacji (w tym także znajdujących się na nośnikach papierowych) przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi, oraz zniszczeniem;
   3) wykonywania aktualizacji oprogramowania urządzeń mobilnych;
   4) instalacji oprogramowania umożliwiającego zdalne usunięcie danych;
   5) instalowania i korzystania na urządzeniach mobilnych wyłącznie z legalnych aplikacji mobilnych;
   6) korzystania z urządzeń mobilnych z zainstalowanym sprawdzonym oprogramowaniem antywirusowym;
2. Użytkownikom urządzeń mobilnych służących do przetwarzania danych osobowych zabrania się:
   1) udostępniania urządzenia osobom nieupoważnionym;
   2) korzystania z urządzeń w warunkach mogących powodować ich uszkodzenie;
   3) łączenia się z siecią publiczną poprzez niezabezpieczone łącza (np. sieć WIFI bez hasła);
   4) wykorzystywania urządzenia do celów prywatnych w trakcie wykorzystywania konta użytkownika przeznaczonego do wykonywania obowiązków służbowych;

§ 4.

Użytkownicy prywatnych urządzeń mobilnych służących do przetwarzania danych osobowych poza obszarem Administratora Danych Osobowych zobowiązani są natychmiastowo tj. do 5 godzin od zaistniałej sytuacji powiadomić Dyrektora lub Inspektora Ochrony Danych w przypadku, kiedy urządzenie:

1) ulegnie uszkodzeniu lub zniszczeniu (w tym zostanie zainfekowane wirusem);
2) zostanie zgubione;
3) zostanie skradzione.

DYREKTOR
Szkoły Podstawowej w Starkowie
mgr Beata Kiedrowska

Szkoła Podstawowa
im. Zjednoczonej Europy w Starkowie
Starkowo 10, 77-235 Trzebielino
Regon 367997167, tel. 598580077