Procedura rozpoczynania, zawieszania i kończenia pracy w systemach informatycznych stosowanych w Szkole Podstawowej im. ks. Jana Twardowskiego w Powidzku

§ 1 Cel i zakres stosowania procedury

1. Celem procedury jest określenie zasad rozpoczynania, zawieszania i kończenia pracy w systemach informatycznych przetwarzających informacje, które podlegają ochronie.
2. Procedura przeznaczona jest dla wszystkich użytkowników systemów informatycznych (nauczyciele, pracownicy administracyjni).

§ 2 Postanowienia ogólne

1. Warunkiem zapewnienia bezpieczeństwa przetwarzania danych jest kontrola dostępu do pomieszczeń stanowiących obszar przetwarzania.
2. Pomieszczenia, w których znajdują się sprzęt komputerowy powinny być zamknięte na klucz podczas nieobecności pracowników (dotyczy również nieobecności w ciągu dnia pracy), a dostęp do nich mogą posiadać wyłącznie osoby do tego upoważnione.
3. Przebywanie osób nieuprawnionych w wyżej wymienionych pomieszczeniach jest dopuszczalne jedynie w obecności osoby upoważnionej.
4. Klucze do pomieszczeń należy przechowywać w sposób uniemożliwiający ich pobranie osobom nieuprawnionym.
5. Monitory stacji roboczych powinny być ustawione w sposób uniemożliwiający wgląd do danych wyświetlanych na ekranie osobom do tego nieuprawnionym.
6. Dokumenty oraz nośniki informacji, które zawierają dane osobowe przechowuje się w szafach zamykanych na klucz.
7. W przypadku stwierdzenia śladów nieuprawnionego wejścia do pomieszczenia zlokalizowanego w obszarze przetwarzania danych osobowych należy powiadomić dyrektora szkoły.

§ 3 Rozpoczęcie pracy

1. Po włączeniu komputera użytkownik loguje się do systemu informatycznego za pomocą swoich danych uwierzytelniających, zgodnie z zapisami Procedury uwierzytelniania użytkowników oraz zarządzania identyfikatorami i hasłami.
2. W trakcie procesu uwierzytelniania dostępu do systemu użytkownik zobowiązany jest do stosowania poniższych zasad bezpieczeństwa:
   a) prawidłowego wprowadzenia danych uwierzytelniających, w sposób uniemożliwiający podejrzenie ich przez osoby nieupoważnione;
   b) uważnego czytania wszystkich ewentualnych komunikatów, które zostaną wyświetlone na ekranie monitora i odpowiedniego reagowania na nie;
   c) korzystania tylko i wyłącznie z danych uwierzytelniających, które zostały mu przydzielone.
3. Dostęp do zasobów systemu powinien być wykorzystywany wyłącznie do celów służbowych i na czas niezbędny do ich wykonywania. W razie wystąpienia nieprawidłowości, w sytuacji podejrzenia naruszenia bezpieczeństwa systemu należy powiadomić bezpośredniego przełożonego oraz postępować zgodnie z Instrukcją postępowania w przypadku naruszeń w ochronie danych osobowych.

§ 4 Zawieszanie i zakończenie pracy

1. Zabrania się pozostawiania bez nadzoru stanowiska pracy, na którym użytkownik zalogował się do systemu informatycznego.

2. W przypadku konieczności zawieszenia pracy w systemie należy wylogować się z systemu lub zabezpieczyć komputer poprzez zablokowanie komputera (np.: wciskając jednocześnie na klawiaturze klawisze Win+ L).
3. Należy bezwzględnie stosować wygaszacze ekranów, na wszystkich stanowiskach komputerowych służących do przetwarzania danych. Wygaszacze powinny być uruchamiane automatycznie i zabezpieczone hasłem. Czas automatycznego uruchomienia wygaszacza nie dłuższy niż 7 min.
4. W pracy z systemem należy przestrzegać zasady „czystego biurka", „czystego ekranu" oraz „czystej drukarki/kserokopiarki".
5. Kończąc pracę w systemie użytkownik zobowiązany jest do prawidłowego wylogowania się z systemu oraz prawidłowego wyłączenia sprzętu komputerowego. Nieprawidłowe zamknięcie systemu (np. poprzez wyłączenie stacji roboczej przyciskiem zasilania lub odłączenie kabla zasilającego) może doprowadzić do utraty wprowadzanych danych. W przypadku nieprawidłowego zamknięcia aplikacji systemu dane niezatwierdzone przez użytkownika zostaną utracone. Tak zamknięta sesja może doprowadzić do utraty wprowadzanych danych, za co odpowiedzialność ponosi użytkownik.
6. Przed opuszczeniem pomieszczenia należy sprawdzić jego stan, a także czy wszystkie urządzenia elektryczne zostały wyłączone i czy wszystkie szafy zostały odpowiednio zamknięte oraz czy zamknięto okna.
7. W uzasadnionych przypadkach dopuszcza się pozostawienie włączonego komputera po godzinach pracy, przy jednoczesnym jego zablokowaniu i zabezpieczeniu dostępu do pomieszczenia.

Powidzko, 25.03.2020 r.

Zaopiniował: Administrator danych:

....
(Inspektor Ochrony Danych Osobowych) (Dyrektor szkoły)