

Regulamin szkolnej sieci komputerowej GIMKONST i polityka bezpieczeństwa

I. Pojęcia wstępne

1. Ile razy w regulaminie jest mowa o:
 - szkole* – rozumie się Gimnazjum Nr 1 w Konstancynie Łódzkim,
 - dyrektorze* – rozumie się dyrektora Gimnazjum Nr 1,
 - użytkownika* – rozumie się ucznia lub pracownika Gimnazjum Nr 1,
 - zbiorze danych osobowych* - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym,
 - dane osobowe* – rozumie się każde informacje dotyczące osoby fizycznej pozwalająca określić jej tożsamość,
 - przetwarzaniu danych* – rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie,
 - zabezpieczeniu danych w systemie informatycznym* – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
 - usuwaniu danych* – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację,
 - system informatyczny* – system sprzętowo - programowy przetwarzający dane,
 - administratorze danych osobowych*– rozumie się dyrektora szkoły,
 - administratorze systemu* – rozumie się osobę odpowiedzialną za sprawne funkcjonowanie systemu informatycznego,
 - administrator bezpieczeństwa informacji* – każdą osobę odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym,
 - stronie internetowej* – rozumie się serwis internetowy Gimnazjum Nr 1 znajdujący się pod adresem <http://www.gimkonst.pl/>,
 - sieci* – rozumie się sprzęt komputerowy wraz z infrastrukturą sieciową znajdującą się w budynku szkoły,
 - koncie* – rozumie się udostępnione usługi dla użytkownika w zasobach sieci.

II. Postanowienia ogólne

1. Regulamin niniejszy ustala zasady funkcjonowania sieci komputerowej w Gimnazjum Nr 1.
2. Podstawową rolą sieci jest wspomoczenie procesu dydaktycznego i wychowawczego, administrowanie i zarządzanie szkołą oraz zapewnienie bezpiecznego przetwarzania danych w tym szczególnie danych osobowych.
3. Sieć tworzy:
 - a) administrator sieci,
 - b) administrator danych,
 - c) administrator bezpieczeństwa informacji,
 - d) użytkownicy,
 - e) komputery i inny sprzęt komputerowy,
 - d) infrastruktura sieciowa.
4. Tryb zmiany regulaminu określają odrębne przepisy.

III. Administrator systemu i administrator bezpieczeństwa informacji

1. Administratora systemu powołuje i odwołuje dyrektor szkoły.
2. Administrator systemu podlega dyrektorowi szkoły.
3. Administrator systemu nadzoruje i zarządza pracą sieci.
4. Administrator systemu może, za zgodą dyrektora, przekazać część uprawnień i zadań osobie trzeciej w ściśle określonym zakresie i trybie.
5. Do jego obowiązków należy:
 - a) organizowanie serwisu sprzętu komputerowego
 - b) nadzór nad instalacją, konfiguracją i utrzymaniem w sprawności sprzętu komputerowego i oprogramowania w szkole, a w szczególności oprogramowania systemowego.
 - c) nadzór nad instalacją, konfiguracją i utrzymaniem w sprawności aplikacji zainstalowanych u użytkowników.
 - d) organizowanie środowiska sieci lokalnej i Internetu.
 - e) utrzymywanie w sprawności urządzeń komputerowej komunikacji sieciowej.
 - f) utrzymywanie w sprawności serwerów sieci komputerowej.
 - g) zakładanie i utrzymanie w sprawności kont użytkowników.
 - h) instalowanie oprogramowania w sieci.
 - i) organizacja zabezpieczeń, okresowa archiwizacja zasobów, kontrola przeciwwirusowa.
 - j) udzielanie pomocy użytkownikom w zakresie obsługi sprzętu i sieci.
 - k) udział w planowaniu rozbudowy struktury sieci.
 - l) wykonywanie innych doraźnych prac na rzecz systemu informatycznego szkoły.
 - m) wykonywanie w miarę możliwości napraw sprzętu.
 - n) aktualizowanie strony internetowej.
 - o) prowadzenie dokumentacji licencyjnej sprzętu komputerowego i oprogramowania.
 - p) prowadzenie podręcznej biblioteki specjalistycznej.
6. Administrator systemu może być jednocześnie administratorem bezpieczeństwa informacji.
7. Administrator bezpieczeństwa informacji jest odpowiedzialny za:
 - a) nadzoruje bezpieczeństwo systemów,
 - b) nadzoruje przestrzeganie obowiązujących procedur,
 - c) weryfikuje listę autoryzowanych użytkowników systemów informatycznych,
 - d) doradza użytkownikom w zakresie bezpieczeństwa,
 - e) zapewnia, aby cały personel posiadający dostęp do systemu posiadał stosowne zezwolenia oraz był przeszkolony w zakresie obowiązujących regulacji bezpieczeństwa,
 - f) przygotowuje i prowadzi „Ewidencja osób biorących udział w przetwarzaniu danych osobowych” i gromadzi upoważnienia do pracy z systemami informatycznymi,
 - g) prowadzi kontrole w zakresie bezpieczeństwa,
 - h) przygotowuje wnioski pokontrolne dla administratora.

IV. Użytkownik sieci

1. Ze sprzętu komputerowego mogą korzystać uczniowie i pracownicy szkoły.

2. Sprzęt komputerowy może być wykorzystywany jedynie w związku wykonywaniem zadań statutowych szkoły zgodnie z obowiązującymi przepisami prawa.
3. Użytkownik jest zobowiązany do ochrony danych osobowych zgodnie z odrębnymi przepisami.
4. Zabrania się korzystania z oprogramowania komputerowego do używania, którego szkoła nie jest uprawniona.
5. Zabrania się niezgodnego z prawem korzystania, rozpowszechniania, utrwalania, pozyskiwania lub zwielokrotniania oprogramowania komputerowego.
6. Użytkownik jest zobowiązany właściwie zalogować się do systemu.
7. Praca z własnymi danymi wymaga sprawdzenia nośnika na obecność wirusów.
8. Po zakończeniu pracy z komputerem należy usunąć zainstalowane w czasie sesji własne pliki.
9. Użytkownik jest zobowiązany informować administratora sieci o wszystkich nieprawidłowościach w funkcjonowaniu sieci i sprzętu.
10. Użytkownik jest zobowiązany dbać o szkolny sprzęt komputerowy oraz infrastrukturę sieciową.
11. Zabronione jest przesyłanie, udostępnianie oraz propagowanie w jakiegokolwiek formie treści obraźliwych lub obscenicznym oraz materiałów niezgodnych z polskim prawem.
12. Zabronione jest wykorzystywanie sieci w celu:
 - a) podejmowania prób nie uprawnionego dostępu do komputerów w sieci lokalnej lub Internecie.
 - b) przechwytywanie danych obecnych w sieci lub Internecie,
 - c) usuwanie lub edycja danych, których nie jest się właścicielem,
 - d) utrudniania pracy innym użytkownikom,
 - e) rozsyłania wirusów, robaków internetowych.
13. Zabronione jest jedzenie i picie w trakcie pracy z komputerem

V. Konta użytkowników

1. Konto na szkolnym serwerze internetowym może otrzymać:
 - a) uczeń szkoły,
 - b) pracownik,
 - c) absolwent szkoły.
2. Konto zakłada się na ustny wniosek zainteresowanego.
3. Administrator może omówić założenia konta podając przyczynę takiej decyzji.
4. Jednej osobie przysługuje jedno konto.
5. Właściciel konta odpowiada za wszystkie operacje podejmowane za jego pomocą.
6. Zabrania się udostępniania własnego konta osobom trzecim.
7. Właściciel konta ma prawo do następujących usług:
 - a) strony WWW,
 - b) skrzynki pocztowej.
8. Strony WWW i skrzynki pocztowe mogą służyć jedynie celom edukacyjnym.
9. Właściciel strony WWW odpowiada za treści zamieszczane we własnym serwisie.
10. Konto pracownika wygasa z dniem rozwiązania umowy o pracę.
11. Prawo do konta może wygasnąć na skutek naruszenia postanowień niniejszego regulaminu.

VI. Polityka bezpieczeństwa w sieci

1. Celem opracowania polityki bezpieczeństwa jest ochrona przed niepożądanym dostępem do:
 - systemu informatycznego oraz informacji udostępnianych z jego wykorzystaniem,
 - informacji zgromadzonych, przetwarzanych w formie tradycyjnej.
2. Zasady polityki bezpieczeństwa reguluje Instrukcja obsługi systemu informatycznego przetwarzania danych osobowych stanowiący załącznik nr 3.
3. Każda zainteresowana osoba ma prawo wystąpić do administratora danych z wnioskiem o udostępnienie danych ze zbioru danych osobowych. Wniosek jest załącznikiem nr 13.
4. Użytkownik jest zobowiązany powiadomić administratora o zaobserwowanych zjawiskach mających wpływ na bezpieczeństwo sieci.
5. Zabronione jest niezgodne z przeznaczeniem wykorzystywanie sieci.
6. W przypadku nagminnego naruszania regulaminu sieci przez użytkownika administrator może w kolejności:
 - a) udzielić ostrzeżenia,
 - b) poinformować dyrektora o zaistniałej sytuacji,
 - c) zablokować konto lub sprzęt
 - d) usunąć konto.