

# REGULAMIN KORZYSTANIA Z ZASOBÓW INFORMATYCZNYCH

## § 1. WSTĘP

1. Organizacja chroni przynależne jej aktywa informatyczne (włączając sprzęt komputerowy, oprogramowanie, sieci, system telefoniczny) przed nieautoryzowanym oraz niewłaściwym użytkowaniem.
2. Dla celów niniejszego dokumentu o nazwie: „Regulamin korzystania z zasobów informatycznych” wprowadza się nazwę skróconą tj.: „Regulamin”
3. Niniejszy „Regulamin” jest skierowany do osób wykonujących pracę na rzecz organizacji na podstawie umów cywilnoprawnych i kodeksu pracy zwanych dalej Użytkownikami.
4. Niniejszy regulamin ma na celu zakomunikowanie Użytkownikom w sposób przejrzysty zasad korzystania z infrastruktury IT organizacji.

## § 2. ZASOBY

1. Organizacja jest właścicielem aktywów podstawowych i wspierających takich jak:
  - 1) **informacje** - obejmują dane osobowe, które organizacja przetwarza w związku z prowadzoną działalnością; informacje niezbędne do osiągnięcia celów organizacji,
  - 2) **operacje przetwarzania** - czynności w procesie przetwarzania danych osobowych, które organizacja jest zobowiązana podejmować/utrzymywać, by osiągać cele strategiczne jednostki przy jednoczesnym zapewnieniu bezpieczeństwa przetwarzanych informacji w organizacji.
  - 3) **sprzęt** - obejmuje przenośne oraz stacjonarne urządzenia komputerowe, urządzenia serwerowe, urządzenia peryferyjne (drukarki czy wymienny napęd dyskowy),
  - 4) **nośniki danych (papierowe) zawierające dane osobowe** - dokumentacja zawierająca treści o charakterze osobowym,
  - 5) **nośniki danych (elektroniczne)** - z racji swojego przeznaczenia mogą być podłączone do urządzenia komputerowego w celu przygotowania danych osobowych do przetwarzania (pendrive, płyta CD/DVD/BD, wymienny dysk twardy),
  - 6) **oprogramowanie** - obejmuje wszystkie programy, dzięki którym bądź w oparciu o nie organizacja przetwarza dane osobowe. W zakresie oprogramowania uwzględnia się system operacyjny, oprogramowanie uzupełniające usługi systemu operacyjnego, oprogramowanie służące do obsługi poczty elektronicznej czy bazy danych, standardowe i dedykowane aplikacje biznesowe np. oprogramowanie księgowo, oprogramowanie służące do obsługi Klientów, pracowników organizacji.
  - 7) **okablowanie** - sieć, którą należy rozumieć przez pryzmat urządzenia używanego do połączenia wielu komputerów i elementów systemu informacyjnego,
  - 8) **personel** – osoby zaangażowane w proces przetwarzania danych osobowych oraz obsługę systemu informacyjnego. Do personelu zaliczamy kierownictwo, osoby upoważnione do przetwarzania danych, osoby, którym nadano uprawnienia do pracy w programach dziedzicznych bazodanowych, osoby, które mają w zakresie swoich obowiązków mają między innymi konieczność utrzymania systemu informacyjnego oraz twórców oprogramowania,
  - 9) **lokalizacja** - siedziba, ale również środowisko zewnętrzne. Siedziba organizacji odnosi się do budynków, jakie organizacja zajmuje oraz wszystkich obszarów przetwarzania wewnątrz budynków. Siedziba jest istotna ze względu na jej położenie geograficzne, obszar miejski, przestrzeń publiczną.

## § 3. UPRAWNIENIA

1. Każdy Użytkownik posiada nadane uprawnienia do systemów informatycznych określające poziom i sposób dostępu do danych organizacji.

2. Procedura nadania / modyfikacji / usunięcia uprawnień wykonywana jest poprzez „Obiegową kartę uprawnień” wnioskowaną przez przełożonego i zatwierdzaną każdorazowo przez Administratora.

#### § 4. OGRANICZENIA

1. Zabrania się Użytkownikom organizacji:
  - 1) samodzielnej naprawy, przeróbki, rozbudowy lub ingerencji w konfigurację sprzętu komputerowego oraz systemów informatycznych,
  - 2) instalowania lub usuwania oprogramowania bez konsultacji z Administratorem lub Administratorem Systemów Informatycznych,
  - 3) wykorzystywania sieci organizacji do nielegalnego ściągania materiałów chronionych prawem autorskim, oraz przechowywania w zasobach informatycznych organizacji takich materiałów,
  - 4) przesyłania danych i dokumentów organizacji przez komunikatory internetowe i sieci p2p,
  - 5) korzystania w trakcie pracy z serwisów ewidentnie nie związanych w zakresie wykonywanych obowiązków służbowych (np. serwisy randkowe, pornograficzne oraz udostępniające treści zakazane prawem lub treści chronione prawem autorskim),
  - 6) podłączania do gniazdek lub listw zasilających sprzęt komputerowy urządzeń o dużym poborze mocy, takich jak: czajniki elektryczne, grzejniki itp.,
  - 7) usuwania lub przerabiania oznaczeń z numerami inwentarzowymi, licencyjnymi lub innymi, którymi sprzęt został oznaczony,
  - 8) zmiany lokalizacji sprzętu komputerowego bez uzgodnienia z Administratorem Systemu Informatycznego lub Administratorem.

#### § 5. BEZPIECZEŃSTWO

1. Wszystkich Użytkowników obowiązuje Polityka Bezpieczeństwa Informacji.
2. Użytkownicy są zobowiązani do zachowania poufności swoich haseł komputerowych. Hasło powinno się składać z minimum 8 znaków.
3. Użytkownicy nie powinni zapisywać swoich haseł w pisemnej lub elektronicznej postaci.
4. Zabrania się nieautoryzowanego używania identyfikacji systemowej, loginów czy przywilejów przypisanych do loginów dla celów innych niż służbowe.
5. Użytkownicy, którzy usiłują odkryć hasła, uzyskać dostęp do ograniczonych zasobów komputerowych naruszają niniejszy regulamin i narażają się na odpowiedzialność w tym zakresie.
6. Zabrania się Użytkownikom nieautoryzowanego dostępu i modyfikacji plików komputerowych nie będących ich własnością, nawet, jeśli nie ma ograniczenia dostępu lub nie ma ochrony pliku. Użytkownik nie ma pozwolenia na dostęp lub modyfikację takich plików, chyba, że posiada stosowne zezwolenie od właściciela pliku. Taki dostęp jest wykroczeniem, jest uważany za nieetyczny i może spowodować pociągnięcie Użytkownika do odpowiedzialności. Jeśli Użytkownik nie jest pewien, czy ma właściwe prawa dostępu do plików, powinien skonsultować się ze swoim przełożonym.
7. Użytkownicy, którzy przyczyniają się do dostępu do chronionych zasobów informatycznych organizacji przez nieuprawnione osoby naruszają niniejszy regulamin.
8. Użytkownicy mają obowiązek zgłaszać wszelkie sytuacje, które wskazują potencjalne ryzyko lub naruszenie bezpieczeństwa zasobów informatycznych bezpośrednio do Administratora i/lub Administratora Systemu Informatycznego i/lub Inspektora Ochrony Danych.

#### § 6. ODPOWIEDZIALNOŚĆ

1. Użytkownicy odpowiadają za powierzony im sprzęt komputerowy. Mają obowiązek chronić go przed negatywnym wpływem czynników zewnętrznych, zniszczeniem, kradzieżą, utratą, oraz modyfikacją lub skasowaniem danych przez osoby nieuprawnione.

2. Użytkownicy mają obowiązek używania zasobów informatycznych organizacji zgodnie z ich przeznaczeniem, w sposób umiętny i wydajny, w celu osiągnięcia celów służbowych.
3. Świadoma działalność użytkowników o charakterze dywersyjnym, mająca na celu zakłócenie normalnej pracy w zasobach informatycznych organizacji, stanowi poważne naruszenie niniejszego regulaminu i może spowodować pociągnięcie użytkownika do odpowiedzialności oraz inne sankcje prawne.

## **§ 7. POCZTA ELEKTRONICZNA**

1. Do obsługi służbowych wiadomości poczty elektronicznej, Użytkownik powinien posługiwać się kontem pocztowym będącym własnością organizacji, obsługiwany przez wskazane przez organizację programy pocztowe.
2. Użytkownik ma obowiązek dołożyć wszelkich starań, by przy przesyłaniu wiadomości poczty elektronicznej, programy pasożytnicze i niebezpieczne załączniki nie trafiły do systemów organizacji lub systemów adresatów tych wiadomości.
3. Użytkownik nie wysyła e-mail zbiorowych tj. jedna wiadomość do wielu adresatów jednocześnie poprzez „Wyślij do” ale poprzez „Wyślij ukrytą kopię do”.
4. Zabrania się Użytkownikowi automatycznego przekierowywania służbowej poczty elektronicznej na zewnętrzne konta nie będące kontami służbowymi. Zakaz dotyczy również automatycznego pobierania poczty służbowej poprzez konta nie będące kontami służbowymi organizacji.
5. Użytkownik powinien szanować przydzielony służbowy adres poczty elektronicznej, w miarę możliwości ograniczyć podawanie go na stronach o wątpliwym poziomie zaufania. Wykradnięcie adresu przez systemy spamujące jest nieodwracalne i naraża systemy antyspamowe organizacji na duże obciążenie.

## **§ 8. ZGŁASZANIE I USUWANIE USTEREK**

1. Problemy ze sprzętem komputerowym lub systemem informatycznym należy zgłosić do Administratora lub Administratora Systemu Informatycznego.