



ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

PRYWATNOŚĆ KONT W SYSTEMACH INFORMATYCZNYCH



**MATERIAŁ SZKOLENIOWY PRZYGOTOWANY PRZEZ CZŁONKÓW
KOMISJI DS. OCHRONY DANYCH OSOBOWYCH DZIAŁAJĄCEJ PRZY ŚZGiP (7/7)**



Prywatność kont w systemach informatycznych

Każdy użytkownik komputera przed przystąpieniem do pracy otrzymuje część przestrzeni w systemie informatycznym czyli konto użytkownika. Wraz z kontem otrzymujemy także login, czyli indywidualną nazwę użytkownika, która jest indywidualnym, unikalnym identyfikatorem każdego użytkownika systemu.

Po co taka indywidualizacja kont?

Dla zapewnienia bezpieczeństwa danych Urzędu i równocześnie zwiększenia Państwu komfortu pracy.

Dzięki takiemu rozwiązaniu możliwa jest identyfikacja i rozliczalność ponieważ wiadomo, kto, kiedy i jakie działania wykonał w systemie informatycznym Urzędu. Ponadto indywidualizacja konta sprawia, że pracujemy tylko w ramach przydzielonych nam zasobów, eliminując ryzyko nawet niezamierzonej ingerencji w pracę innych użytkowników tego samego systemu.

Jeśli dobrowolnie zrezygnujemy z tego komfortu udostępniając komuś naszą przestrzeń w systemie np. poprzez ujawnienie hasła dostępu lub wręcz udostępnimy własne konto, to świadomie ryzykujemy pełną odpowiedzialnością za wszystko, co ktoś inny posługując się naszym loginem, dokona w systemie Urzędu.



**Aby uchronić Państwa przed popełnieniem błędów, wprowadza
się do stosowania**

ZASADĘ PRYWATNOŚCI KONT W SYSTEMACH

Zasada prywatności kont w systemach – każdy użytkownik systemu informatycznego jest zobowiązany do pracy jedynie na przypisanych mu kontach użytkownika, które jednoznacznie go identyfikują i wyróżniają. Zabronione jest udostępnianie konta użytkownika systemu informatycznego innym osobom, które nie zostały do nich przypisane.

O CZYM NALEŻY PAMIĘTAĆ W CODZIENNEJ PRACY?

- Jak każdy pracownik mogę pracować wyłącznie na swoim koncie użytkownika, do którego nadano mi dostęp.
- Moje konto jest tylko moje i tylko ja mogę na nim pracować i nie udostępniam go innej osobie. To tak samo oczywiste, jak to, że nie oddaję osobom postronnym dowodu osobistego lub konta w banku do dyspozycji.
- Moje indywidualne konto użytkownika zapewnia mi komfort pracy i bezpieczeństwo ponieważ pozwala na identyfikację mojej aktywności w systemie informatycznym Urzędu, dzięki czemu odpowiadam za siebie i efekty swojej pracy. Login jest jak „odciski palców” które zostawiam w systemie informatycznym.
- Aby chronić konto nie przekazuję hasła do logowania innej osobie, nawet zaprzyjaźnionej i zaufanej. Dzięki temu mam pewność, że wszelka działalność w systemie informatycznym Urzędu jest faktycznie moja ponieważ mam dowód na to w postaci podpisu, jakim jest mój login. Jest to również istotne przy identyfikacji „sprawcy” incydentu.
- Jeśli do mojego konta otrzymałem podpis elektroniczny, pamiętam, że jest po to, by identyfikować mnie jako konkretną osobę, więc nie udostępniam innym osobom karty i hasła umożliwiającego złożenie podpisu elektronicznego. Podpis oznacza przecież osobistą odpowiedzialność za treść podpisanego dokumentu. To tak, jakby podpisać weksel, a sumę pozostawić komuś innemu do wypełnienia.
- Jeśli wejście do pomieszczenia, w którym pracuję chronione jest kodem, nie ujawniam kodu osobom postronnym. W przypadku stwierdzenia incydentu odpowiedzialność poniosą osoby, które znały kod, a nie te, trudne do ustalenia, którym kod ujawniono.
- Stosując się do powyższych zasad mam pewność, że nikt nie zrobi w moim imieniu czegoś niechcianego w systemie informatycznym Urzędu.



ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

Dziękujemy za uwagę.

Komisja ds. Ochrony Danych Osobowych

<https://silesia.org.pl/struktura/komisje/komisja-ds-ochrony-danych-osobowych/>

