

Praca w systemach, na komputerach i innych urządzeniach

Dokument opisuje sposób bezpiecznej pracy w systemach informatycznych, programach lub aplikacjach, a także na sprzęcie komputerowym (w tym urządzeniach przenośnych).

Spis treści

1. Wstęp	2
2. Potwierdzanie tożsamości	2
3. Zakres dostępu	3
4. Rozpoczynanie i kończenie pracy	3
5. Praca na plikach i programach	3
6. Internet	3
7. Nośniki danych	4
8. Poczta elektroniczna	4
9. Przesyłanie plików zawierających dane osobowe lub informacje poufne	5
10. Urządzenia przenośne	5
11. Odpowiedzialność użytkownika	6
12. Postanowienia końcowe	6

1. Wstęp

Do przestrzegania zaleceń opisanych w niniejszym dokumencie zobowiązane są wszystkie osoby, współpracujące z ADO (niezależnie od stażu pracy, zajmowanego stanowiska lub podstawy współpracy), które w ramach obowiązków służbowych pracują w systemach informatycznych, na komputerach lub innych urządzeniach, w tym urządzeniach przenośnych.

2. Potwierdzanie tożsamości

1. Podstawową metodą weryfikacji tożsamości użytkownika komputera lub systemu są dane dostępne: nazwa użytkownika (login) i hasło.
2. Login i pierwsze hasło do komputera lub systemu są nadawane użytkownikowi przez IT lub – w uzasadnionych przypadkach – użytkownik ustala je samodzielnie. Hasło nadane przez IT użytkownik jest zobowiązany niezwłocznie zmienić na własne.
3. Użytkownik jest zobowiązany do zachowania loginu i hasła w tajemnicy. W szczególności oznacza to, że użytkownik:
 - 1) nie ujawnia ich przełożonym, współpracownikom, podwładnym, kontrahentom, osobom korzystającym z usług ADO itd.,
 - 2) nie zapisuje ich w sposób umożliwiający dostęp do nich osobom nieupoważnionym (np. przez zapisanie na kartce przyklejonej do monitora lub pod klawiaturą),
 - 3) nie może wykorzystywać loginów i haseł innych osób.
4. Użytkownik jest zobowiązany do zmiany hasła zgodnie z przyjętą u ADO częstotliwością. Zmiana hasła następuje niezależnie od tego, czy komputer lub system przypomina użytkownikowi o zmianie, czy nie.
5. Hasło powinno spełniać wymogi określone przez ADO lub – jeśli takie nie zostały określone wskazane poniżej:
 - 1) długość: nie krótsze niż 8 (osiem) znaków,
 - 2) stosowane znaki alfanumeryczne: co najmniej jedna mała litera, co najmniej jedna duża litera, co najmniej jedna cyfra lub znak specjalny (!@#\$%^&* itp.),
 - 3) wykluczone elementy: hasło nie może zawierać jako jedynego składnika elementu możliwego do odgadnięcia lub weryfikacji przez osoby nieupoważnione (imion, nazwisk, numerów telefonów, numerów rejestracyjnych pojazdu, nazw drużyn sportowych, danych o osobach bliskich itd.); hasło nie może także zawierać elementów łatwych do odgadnięcia (np. zaq12wsx, asdfghjkl, 12345678 itd.),
 - 4) powtarzalność: przy ustawianiu hasła użytkownikowi nie wolno używać wcześniej stosowanych haseł.
6. Wymogi wskazane w ust. 5 powyżej są spełniane niezależnie od tego, czy komputer lub system przypomina użytkownikowi o zmianie, czy nie.
7. W razie:
 - 1) stwierdzenia lub podejrzenia, że inna osoba weszła w posiadanie loginu lub hasła,
 - 2) zapomnienia loginu lub hasła,
 - 3) zablokowania dostępu do komputera lub systemu związanego z wielokrotnym wprowadzeniem błędnego loginu lub hasła– użytkownik jest zobowiązany do niezwłocznego zawiadomienia o tym IT i postępowania zgodnie z jego poleceniami.
8. Zalecenia dotyczące loginu i hasła stosuje się odpowiednio wobec innych metod potwierdzania tożsamości, jeśli są stosowane u ADO.

3. Zakres dostępu

1. O ile nie jest to niezbędne dla wykonywania obowiązków użytkownika, powinien on pracować na standardowym koncie użytkownika systemu operacyjnego, pozbawionym uprawnień administracyjnych.
2. Użytkownik pracuje na tych plikach, modułach lub częściach aplikacji, programów lub systemów, które są niezbędne dla wykonywania jego obowiązków służbowych.
3. Użytkownik nie podejmuje działań mających na celu nieautoryzowaną zmianę dostępu, w szczególności poprzez przełamywanie zabezpieczeń lub wykorzystywanie luk w zabezpieczeniach.
4. W razie stwierdzenia zmiany w zakresie dostępu (np. utraty dostępu do dotychczas stosowanego modułu programu) lub innego niestandardowego działania systemu (np. wyświetlenia komunikatu błędu) użytkownik jest zobowiązany do niezwłocznego zawiadomienia o tym IT i postępowania zgodnie z jego poleceniami.

4. Rozpoczynanie i kończenie pracy

1. Przy wpisywaniu loginu i hasła użytkownik jest zobowiązany upewnić się, czy jego poczynania nie śledzi osoba nieupoważniona, która mogłaby w ten sposób wejść w posiadanie danych dostępowych użytkownika.
2. W razie konieczności przzerwania pracy na komputerze na krótki czas, użytkownik powinien zablokować komputer lub wylogować się z systemu operacyjnego. Takie działanie może być w szczególności wykonane przez wybranie na klawiaturze kombinacji [klawisz Windows] + L (w systemie operacyjnym Windows).
3. Po zakończeniu pracy użytkownik wylogowuje się z aplikacji, systemów lub programów, a następnie wyłącza komputer.

5. Praca na plikach i programach

1. Na komputerach powinny być wykorzystywane jedynie pliki związane z wykonywaniem obowiązków służbowych. O ile ADO nie wskaże inaczej, wykluczone jest wykorzystywanie na komputerach prywatnych plików (zdjęć, filmów, muzyki itp.).
2. Każdy plik pobierany na komputer (z internetu, poczty elektronicznej, nośnika zewnętrznego) musi być przeskanowany zainstalowanym na komputerze programem antywirusowym.
3. Użytkownik nie może zapisywać plików zawierających dane osobowe (zwłaszcza szczególne kategorie danych) bezpośrednio na pulpicie komputera lub dysku twardym komputera. Takie pliki powinny być zapisywane na udostępnionym przez ADO dysku sieciowym.
4. O ile ADO nie wskaże inaczej, zabroniona jest samodzielna instalacja oprogramowania na komputerach przez osoby zatrudnione.
5. W razie stwierdzenia lub podejrzenia, że na komputerze użytkownika znalazło się złośliwe oprogramowanie (wirusy, konie trojańskie itp.), użytkownik jest zobowiązany do niezwłocznego zawiadomienia o tym IT i postępowania zgodnie z jego poleceniami.

6. Internet

1. Użytkownik wykorzystuje internet (strony internetowe, komunikatory, usługi pozwalające na przesyłanie plików itp.) jedynie w celach związanych z wykonywaniem obowiązków służbowych. O ile ADO nie wskaże inaczej, wykluczone jest wykorzystywanie internetu dla celów niezwiązanych z realizacją obowiązków służbowych.
2. W celu zapewnienia bezpieczeństwa informacji, organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkownika udostępnionych użytkownikom

narzędzi pracy, ADO zastrzega sobie prawo monitorowania aktywności użytkowników w internecie. Użytkownicy są o takim monitorowaniu uprzednio informowani.

3. Osoby, które w związku z realizacją obowiązków służbowych używają internetu poza stałym miejscem pracy, zobowiązane są do jego używania w sposób gwarantujący bezpieczeństwo, tj. w szczególności poprzez:
 - 1) wykorzystanie mobilnej transmisji danych z własnego urządzenia przenośnego,
 - 2) wykorzystanie mobilnej transmisji danych z urządzenia przenośnego dla udostępnienia internetu na innym urządzeniu (*tethering*),
 - 3) wykorzystanie technologii VPN dla zabezpieczenia połączenia z internetem,
 - 4) wykorzystywanie godnych zaufania sieci wi-fi.

7. Nośniki danych

1. Wykorzystywanie nośników danych (dyskietek, płyt, pendrive'ów itp.) do przetwarzania danych osobowych jest domyślnie – ze względu na zagrożenie dla poufności lub integralności tych danych – niedozwolone.
2. Użytkownik nie może wykorzystywać dla celów służbowych nośników:
 - 1) niebędących własnością ADO lub
 - 2) które nie zostały (po konsultacji z IT) dopuszczone do wykorzystywania u ADO.
3. Każdy nośnik podłączany lub wprowadzany do komputera musi być przeskanowany zainstalowanym na komputerze programem antywirusowym.
4. Dane osobowe lub informacje poufne na nośniku powinny być zaszyfrowane w sposób skonsultowany lub dopuszczony przez IT.
5. Nośniki danych, zawierające dane osobowe lub informacje poufne, są przechowywane w miejscu, do którego nie mają dostępu osoby nieupoważnione.
6. W razie stwierdzenia:
 - 1) braku możliwości odczytania danych osobowych lub informacji poufnych, zapisanych na nośniku,
 - 2) obecności na nośniku złośliwego oprogramowania- użytkownik niezwłocznie zawiadamia o tym IT i postępuje zgodnie z jego wskazówkami.
7. W razie stwierdzenia zgubienia lub kradzieży nośnika danych, zawierającego dane osobowe lub informacje poufne, użytkownik niezwłocznie zawiadamia o tym ADO i postępuje zgodnie z jego wskazówkami.

8. Poczta elektroniczna

1. Użytkownik wykorzystuje służbowe konto poczty elektronicznej jedynie w celach związanych z wykonywaniem obowiązków służbowych. O ile ADO nie wskaże inaczej, wykluczone jest:
 - 1) wykorzystywanie służbowego konta poczty elektronicznej dla celów niezwiązanych z realizacją obowiązków służbowych,
 - 2) wykorzystywanie prywatnego konta poczty elektronicznej dla celów związanych z realizacją obowiązków służbowych.
2. Użytkownik konta poczty elektronicznej jest odpowiedzialny za wiadomości wysyłane z tego konta.
3. Każdorazowo należy weryfikować nadawcę otrzymanej wiadomości e-mail (osobę fizyczną lub przedstawiciela firmy, urzędu, instytucji itd.) w celu wykluczenia, że podszywa się pod niego osoba nieupoważniona. O podszyciu się pod nadawcę może świadczyć w szczególności:
 - 1) inny niż do tej pory adres e-mail, z którego komunikuje się nadawca,

- 2) błędy ortograficzne, składniowe, merytoryczne w treści wiadomości,
 - 3) treść wiadomości, nakazująca szybkie wykonanie określonego działania (w szczególności kliknięcia w link lub otworzenia załącznika) pod rygorem negatywnych konsekwencji,
 - 4) obecność załącznika niezwiązanego z treścią wiadomości,
 - 5) załącznik w postaci pliku tzw. pliku wykonywalnego (z rozszerzeniem EXE, VB, BAT itd.)
- W celu weryfikacji wiadomości użytkownik powinien w szczególności zawiadomić IT o takiej potrzebie i postępować zgodnie z jego wskazówkami.
4. W razie stwierdzenia, że otrzymana wiadomość stanowi próbę wyłudzenia danych, informacji lub pieniędzy przez podszycie się pod osobę lub instytucję (*phishing*), użytkownik zawiadamia o takiej sytuacji IT oraz postępuje zgodnie z jego wskazówkami.
 5. Przed wysłaniem wiadomości e-mail, w szczególności zawierającej dane osobowe lub informacje poufne, należy upewnić się, czy wskazano właściwy adres e-mail odbiorcy, tj. czy:
 - 1) należy on do osoby lub instytucji zaangażowanej w sprawę będącą przedmiotem wiadomości,
 - 2) nie zawiera on błędów, które mogłyby spowodować, że dane lub informacje trafią do osoby nieupoważnionej.
 6. W przypadku wysyłania wiadomości zawierających dane osobowe lub informacje do wielu odbiorców użytkownik nie może umieszczać ich adresów e-mail w polu „Do” lub „Do wiadomości / DW / CC” (nie jest także dopuszczalne używanie opcji „Odpowiedz wszystkim”). W takiej sytuacji należy umieścić adresy e-mail wszystkich odbiorców w polu „Ukryte do wiadomości / UDW / BCC”.
 7. IT może w uzasadnionych przypadkach nadać dostęp do jednego służbowego konta poczty elektronicznej kilku użytkownikom.

9. Przesyłanie plików zawierających dane osobowe lub informacje poufne

1. Przesyłanie plików zawierających dane osobowe lub informacje poufne odbywa się w sposób zapewniający, że z danymi lub informacjami nie będą mogły się zapoznać osoby nieupoważnione.
2. Przesyłanie plików między osobami zatrudnionymi u ADO może odbywać się w szczególności z wykorzystywaniem służbowej poczty elektronicznej (gdzie ADO ma możliwość wdrożenia adekwatnych środków bezpieczeństwa) lub dysku sieciowego.
3. W przypadku przesyłania plików na zewnątrz zalecane jest ich zaszyfrowanie poprzez:
 - 1) umieszczenie pliku z danymi osobowymi lub informacjami poufnymi w archiwum (7Z, RAR, ZIP itd.)
 - 2) opatrzenie archiwum hasłem spełniającym wymogi opisane w rozdziale 1,
 - 3) wysłanie archiwum za pośrednictwem poczty elektronicznej,
 - 4) przekazanie hasła innym niż poczta elektroniczna kanałem komunikacji (np. SMS-em, w rozmowie telefonicznej itd.).
4. ADO może dopuścić stosowanie innych niż wskazane w ust. 3 powyżej metod szyfrowania.

10. Urządzenia przenośne

1. Osoba zatrudniona u ADO korzysta z urządzeń przenośnych (laptopów, tabletów, iPadów, smartfonów itp.) dla celów służbowych, zachowując następujące środki bezpieczeństwa:
 - 1) do urządzenia zarówno w godzinach pracy, jak i po jej zakończeniu nie mają dostępu osoby nieupoważnione,

- 2) urządzenie jest przechowywane lub transportowane w sposób nienarażający go na przypadkowe lub celowe zniszczenie, uszkodzenie, kradzież lub zgubienie,
 - 3) ekran urządzenia jest ustawiony w sposób, który uniemożliwia osobom postronnym wgląd w treści wyświetlane na ekranie (dla osiągnięcia tego celu dopuszczalne jest także stosowanie filtrów prywatyzujących lub innych dopuszczonych przez ADO rozwiązań).
2. Tablety, iPady, smartfony itp., wykorzystywane dla celów służbowych, są zabezpieczane:
- 1) kodem PIN – używanym w celu rozpoczęcia pracy na urządzeniu po jego włączeniu,
 - 2) dodatkowym zabezpieczeniem (kodem PIN, hasłem, gestem, odciskiem palca itp.) – używanym w celu wznowienia pracy na urządzeniu po jego zablokowaniu lub przerwaniu pracy.
3. W zakresie nieuregulowanym w tym rozdziale osoba zatrudniona stosuje ogólne środki bezpieczeństwa, wskazane w tym dokumencie.

11. Odpowiedzialność użytkownika

1. Każdy użytkownik jest odpowiedzialny za działania podejmowane z jego konta lub sprzętu służbowego, będące konsekwencją nieprzestrzegania wprowadzonych u ADO procedur pracy w systemach, na komputerach i innych urządzeniach.
2. Nieprzestrzeganie obowiązujących u ADO procedur pracy w systemach, na komputerach i innych urządzeniach może być traktowane będzie jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku współpracy na podstawie innej niż stosunek pracy.

12. Postanowienia końcowe

ADO może dopuścić odstępnie od zasad opisanych w niniejszym dokumencie, pod warunkiem dokonania analizy ryzyka związanego z takim odstępstwem oraz wprowadzenia innych rozwiązań, gwarantujących odpowiedni poziom bezpieczeństwa.