

|                                                                                                                                            |                    |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------|
| <br><b>Polityka bezpieczeństwa i poufności informacji</b> | Strona/Stron       | 1/16       |
|                                                                                                                                            | Wydanie            | 1          |
| <b>Dokument stworzył: Marek Garbacz</b><br><b>Zaakceptował: Adam Ogonowski</b>                                                             | Data obowiązywania | 24.06.2024 |
|                                                                                                                                            |                    |            |

## **POLITYKA BEZPIECZEŃSTWA I POUFNOŚCI INFORMACJI**

### **Przedmiot Instrukcji – Polityki bezpieczeństwa i poufności informacji**

Zasady stosowane w Wydawnictwie Jedność / Drukarni DAP w zakresie polityki bezpieczeństwa i poufności informacji.

### **Dotyczy stanowisk**

Wszystkich pracowników Wydawnictwa JEDNOSĆ oraz Drukarni DAP im Adama Półtawskiego w Kielcach

### **Dokumenty związane:**

BHP – Ulotka dla klientów,

BHP – Ulotka dla kierowców i kurierów firm zewnętrznych

Zarządzenie Nr 1/2021 w zakresie bezpieczeństwa informacji

Procedura postępowania dla pracowników ochrony, firmy zewnętrznej oraz etatowych pracowników Wydawnictwa Jedność w Drukarni DAP im Adama Półtawskiego

Zarządzenie Nr 2/2021 z dnia 08.11.2021 do Regulaminu Pracy Wydawnictwa Jedność

|                                                                                                                                            |                    |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------|
| <br><b>Polityka bezpieczeństwa i poufności informacji</b> | Strona/Stron       | 2/16       |
|                                                                                                                                            | Wydanie            | 1          |
| <b>Dokument stworzył: Marek Garbacz</b><br><b>Zaakceptował: Adam Ogonowski</b>                                                             | Data obowiązywania | 24.06.2024 |
|                                                                                                                                            |                    |            |

### **Zadanie jest wykonywane**

Niezwłocznie po zapoznaniu się pracowników, klientów i kooperantów z instrukcją wg daty obowiązywania.

### **Narzędzia i materiały**

Sprzęt komputerowy

Instrukcje

### **Osobiste środki ochrony i szkolenia BHP**



**UWAGA!**

**PRZESTRZEGANIE ZASAD BHP BEZWZGLĘDNIE OBOWIĄZKOWE.**

Przebieg czynności

### **Wykaz załączników:**

Ulotka informacyjna BHP dla klientów

Ulotka informacyjna BHP dla kierowców i kurierów firm zewnętrznych

Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy

|                                                                                                                                            |                    |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------|
| <br><b>Polityka bezpieczeństwa i poufności informacji</b> | Strona/Stron       | 3/16       |
|                                                                                                                                            | Wydanie            | 1          |
| <b>Dokument stworzył: Marek Garbacz</b><br><b>Zaakceptował: Adam Ogonowski</b>                                                             | Data obowiązywania | 24.06.2024 |
|                                                                                                                                            |                    |            |

---

Uwagi

Bezwzględne stosowanie się do zasad opisanych zgodnie z polityką opisaną w instrukcji

Aktualizacja:

### **Definicja poufności i bezpieczeństwa informacji:**

**Poufność** informacji oznacza, że **dostęp do niej jest ograniczony do wybranej grupy osób lub jednostki, które mają odpowiednie uprawnienia do jej przetwarzania**. Celem zapewnienia poufności jest ochrona danych przed dostępem przez osoby do tego nieupoważnione, co pozwala na zachowanie integralności, wiarygodności i poufności informacji.

**Bezpieczeństwo** informacji czasami skracane jest do InfoSec. Choć ja częściej wykorzystuje w rozmowie formę skróconą, bo tak jest wygodniej. Bezpieczeństwo informacji to nie tylko zabezpieczenie informacji przed nieautoryzowanym dostępem. To również część zarządzania ryzykiem związanym z informacjami, która obejmuje zabezpieczenie przeciwko nieautoryzowanemu dostępowi, wykorzystaniu, ujawnieniu, zakłóceniu, modyfikacji, kontroli, zapisywaniu lub niszczeniu informacji.

Osiąga się to poprzez procesy i narzędzia wykorzystane przez organizacje. Mogą mieć zarówno formę fizyczną, jak i elektroniczną. Informacjami mogą być dowolne dane personalne, może to być Twój profil społecznościowy, dane na telefonie, biometryczne, dane konta klienta, dane finansowe lub własność intelektualna [ jak własność naszych klientów ] i tym podobne.

Zagrożenia dla bezpieczeństwa informacji przybierają różne formy, w tym kłęski żywiołowe, awarie serwerów, kradzieże fizyczne i niezabezpieczone, nieświadome podatności na komputerach pracowników. Poleganie na systemach informatycznych sprawia, że bezpieczeństwo informacji staje się kluczowym elementem zarządzania ryzykiem bezpieczeństwa w organizacji.

|                                                                                                                                            |                    |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------|
| <br><b>Polityka bezpieczeństwa i poufności informacji</b> | Strona/Stron       | 4/16       |
|                                                                                                                                            | Wydanie            | 1          |
| <b>Dokument stworzył: Marek Garbacz</b><br><b>Zaakceptował: Adam Ogonowski</b>                                                             | Data obowiązywania | 24.06.2024 |
|                                                                                                                                            |                    |            |

---

Musimy pamiętać iż smartfony, tablety i inne urządzenia mobilne są tak samo „komputerem”, jak i serwer itp.

I wszystkie one są podatne na złośliwe cyberataki, które mogą ułatwić dostęp do poufnych informacji, krytycznych informacji lub zasobów informacyjnych. To, w połączeniu z rosnącą liczbą naruszeń danych, doprowadziło do zwiększonego zapotrzebowania na zaawansowane planowanie ochrony danych i rosnącego zapotrzebowania na specjalistów ds. bezpieczeństwa informacji.

Do najważniejszych wymagań prawnych w zakresie ochrony określonej kategorii informacji należy zaliczyć:

ochronę danych osobowych (klientów, kontrahentów, pracowników, współpracowników),

ochronę tajemnicy przedsiębiorstwa (technologie, strategię, know-how),

ochronę informacji finansowej i podatkowej (finanse, rachunki, faktury, płace),

ochronę informacji niejawnych (tajemnicę państwową)

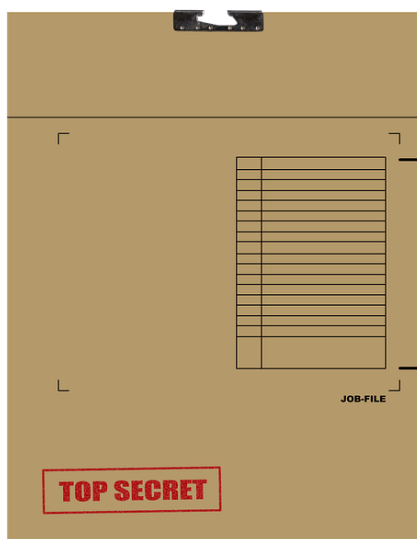
tajemnicę zawodową (lekarską, adwokacką, bankową).

Dane te mogą pochodzić z naszych nośników jak i materiałów drukarskich a następnie intrologatorskich.

Dlatego tak ważne jest by podnosić świadomość naszych pracowników poprzez informacje w czasie spotkań, rozmów, szkolenia oraz tworzenie i zapoznavanie się z politykami, instrukcjami i procedurami np.. postępowania na wypadek wycieku informacji.

|                                                                                                                                            |                    |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------|
| <br><b>Polityka bezpieczeństwa i poufności informacji</b> | Strona/Stron       | 5/16       |
|                                                                                                                                            | Wydanie            | 1          |
| <b>Dokument stworzył: Marek Garbacz</b><br><b>Zaakceptował: Adam Ogonowski</b>                                                             | Data obowiązywania | 24.06.2024 |
|                                                                                                                                            |                    |            |

Dokumenty szczególnie ważne i wrażliwe zawsze powinny być zabezpieczone i opisane np. jak poniżej:



Oczywiście nie chodzi tu o samo oznaczenie, nadmierne ukazanie tego co robimy i jak to powinno wyglądać ale o zaznaczenie i zgodne postępowanie z przyjętymi zasadami. Czasem drobne działania bez zbędnych wydatków na systemy, sejfy itp. Pozwolą nam na uniknięcie problemu i narażenie pracowników firmy na koszty a nawet na utratę klienta.

Podstawowe działania polegające na zabezpieczaniu informacji niejawnych, wrażliwych, poufnych to:

- Niepozostawianie dok na biurku w czasie wizyt osób postronnych lub gości
- Wyłączanie, zabezpieczanie komputera, tableta, telefonu hasłem
- Częste zmiany co około 30 dni hasła na urządzeniu
- Nie prowadzenie rozmów w miejscach publicznych ( stołówka, sala ćwiczeń ) zarówno w firmie jak i poza nią na tematy zawodowe
- Unikanie zbędnych wydruków dok. w formie papierowej
- Przed wysłaniem wiadomości sprawdzenie adresata
- Nie otwieranie podejrzanych i nieznanomych wiadomości
- Unikanie synchronizacji poczty prywatnej ze służbową

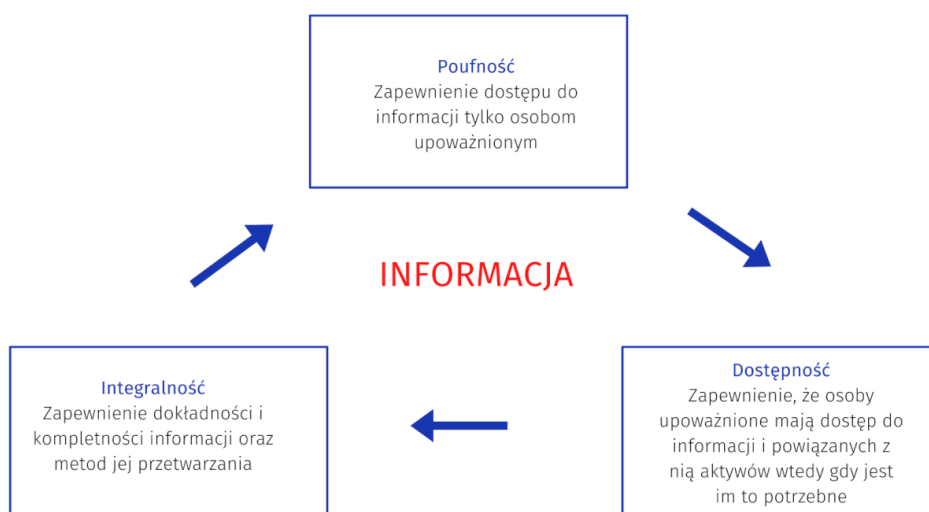
|                                                                                                                                            |                    |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------|
| <br><b>Polityka bezpieczeństwa i poufności informacji</b> | Strona/Stron       | 6/16       |
|                                                                                                                                            | Wydanie            | 1          |
| <b>Dokument stworzył: Marek Garbacz</b><br><b>Zaakceptował: Adam Ogonowski</b>                                                             | Data obowiązywania | 24.06.2024 |
|                                                                                                                                            |                    |            |

**Na rynku istnieje wiele systemów zabezpieczających informacje niejawne ale żaden system nie da nam lepszej gwarancji niż świadomi pracownicy.**

**Systemy zabezpieczeń** to nic innego jak strategia działania, której celem jest zapewnianie właściwej ochrony **informacji**. Idealne strategie to takie które mogą zapewnić ciągłe doskonalenie podjętych działań i procedur w celu optymalizacji ryzyk związanych z naruszeniem poufności.

Innymi słowy polityka, instrukcje bezpieczeństwa informacji i świadomość pracowników mają chronić przed zagrożeniami w sposób, który zapewni organizacji:

- ciągłość prowadzenia działalności
- zminimalizowanie strat
- maksymalizowanie zwrotu nakładów na inwestycje i działania o charakterze biznesowym



|                                                                                                                                            |                    |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------|
| <br><b>Polityka bezpieczeństwa i poufności informacji</b> | Strona/Stron       | 7/16       |
|                                                                                                                                            | Wydanie            | 1          |
| <b>Dokument stworzył: Marek Garbacz</b><br><b>Zaakceptował: Adam Ogonowski</b>                                                             | Data obowiązywania | 24.06.2024 |
|                                                                                                                                            |                    |            |

Kolejnym sposobem poprawy bezpieczeństwa informacji jest norma ISO 27001, która daje możliwości ochrony danych osobowych i przydzielonych zasobów.

PN-EN ISO/IEC 27001:2023-08 to międzynarodowa norma standaryzująca systemy zarządzania bezpieczeństwem informacji. Została ona opracowana na podstawie brytyjskiego standardu BS 7799-2, a jej celem jest dostarczenie wymagań dotyczących ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu pozwalającego na zachowanie bezpieczeństwa danych w każdej z organizacji.

## ZAKRESIE BEZPIECZEŃSTWA INFORMACJI

### Pracownicy

W związku z oczekiwaniami organizacji oraz naszych klientów w zakresie bezpieczeństwa i poufności informacji niejawną decyzją zarządu wprowadzono zakaz używania telefonów, tabletów, komputerów osobistych w obszarze produkcji i innych nośników i urządzeń elektronicznych.

Zabronione jest również w obszarze produkcji robienie zdjęć, nagrywanie, odtwarzanie oraz publikowanie materiałów na w/w urządzeniach elektronicznych lub publikowanie na portalach społecznych.

Używanie telefonów dozwolone jest jedynie:

w pomieszczeniu stołówki pracowniczej, palarni oraz w szatni

W przypadku niezastosowania się do zarządzenia Pracodawca ma prawo nałożyć na Pracownika karę upomnienia/nagany oraz obciążyć go kosztami powstałych strat wobec Wydawnictwa Jedność lub klientów zewnętrznych.

Uporczywe używanie nośników jw., pomimo stosowanych kar, będzie skutkowało rozwiązaniem umowy o pracę

|                                                                                                                                            |                    |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------|
| <br><b>Polityka bezpieczeństwa i poufności informacji</b> | Strona/Stron       | 8/16       |
|                                                                                                                                            | Wydanie            | 1          |
| <b>Dokument stworzył: Marek Garbacz</b><br><b>Zaakceptował: Adam Ogonowski</b>                                                             | Data obowiązywania | 24.06.2024 |
|                                                                                                                                            |                    |            |

Celem tej polityki jest uświadamianie pracowników, ustalenie zasad i wytycznych dotyczących użytkowania mediów społecznościowych po to, aby zagwarantować firmie ochronę w zakresie nieuprawnionego ujawnienia informacji, a pracownikom ochronę dóbr osobistych. Media społecznościowe obejmują wszystkie formy publicznej i niepublicznej komunikacji internetowej. Chodzi zarówno o media istniejące w momencie wprowadzania polityki, jak i te, które zostaną stworzone w przyszłości, w tym między innymi wymienione poniżej:

- serwisy społecznościowe (np. Facebook, LinkedIn, Google+, Yammer),
- serwisy internetowe umożliwiające dzielenie się zdjęciami i filmami video (np. Flickr, YouTube),
- serwisy umożliwiające mikroblogowanie (np. Twitter),
- blogi (np. blogi korporacyjne, prywatne),
- fora i tablice dyskusyjne (np. Yahoo!, grupy dyskusyjne Google),
- serwisy umożliwiające wspólne publikowanie treści (np. Wikipedia),
- serwisy społecznościowe dostarczone pracownikom przez różne firmy w domenie @dap.pl lub innym firmowym adresem).

Jeśli pracownik nie jest pewny, czy platforma lub narzędzie, którego używa, jest medium społecznościowym i tym samym jest objęte tą polityką, powinien skontaktować się z przedstawicielem Działu ds. Personalnych, dyrektorem zarządzającym lub dyrektorem wydawnictwa ks. Leszkiem Skorupą osobiście lub pod adresami:

- [skorupa@jednosc.com.pl](mailto:skorupa@jednosc.com.pl).
- [kadry@jednosc.com.pl](mailto:kadry@jednosc.com.pl)
- [adam.ogonowski@jednosc.com.pl](mailto:adam.ogonowski@jednosc.com.pl)



|                                                                                                                                            |                    |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------|
| <br><b>Polityka bezpieczeństwa i poufności informacji</b> | Strona/Stron       | 9/16       |
|                                                                                                                                            | Wydanie            | 1          |
| <b>Dokument stworzył: Marek Garbacz</b><br><b>Zaakceptował: Adam Ogonowski</b>                                                             | Data obowiązywania | 24.06.2024 |
|                                                                                                                                            |                    |            |

Firma respektuje prawa pracowników do tworzenia i użytkowania mediów społecznościowych, jednak tego typu aktywność musi być realizowana w taki sposób, aby skutecznie chronić reputację i interesy Wydawnictwa Jedność / Drukarni DAP. Ten dokument ma na celu uzupełnienie, a nie zastąpienie istniejących zasad firmy dotyczących poufności, zasad profesjonalnego działania, ochrony dóbr osobistych i innych zasad dotyczących oczekiwanego sposobu zachowania.

**Zastosowanie** Polityka dotyczy wszystkich pracowników Jedność / DAP, we wszystkich lokalizacjach i działach..

**Polityka** Podczas użytkowania mediów społecznościowych pracownicy powinni przestrzegać zasad firmy dotyczących etycznego postępowania oraz innych zasad obowiązujących w Jedność / DAP, włączając zasady niniejszej polityki. Pracownicy powinni mieć na uwadze, że każda ich aktywność w internecie, która niekorzystnie wpływa na ich wydajność pracy, wydajność innych pracowników, interesy klientów, dostawców lub na interesy gospodarcze firmy, może skutkować wszczęciem wobec tych pracowników postępowania dyscyplinarnego ze zwolnieniem włącznie.

**Wytyczne** Poniższe wytyczne dotyczą użytkowania publicznych oraz prywatnych mediów społecznościowych przez pracowników Jedność / DAP, niezależnie od tego, czy używane są one podczas pracy czy w czasie wolnym oraz niezależnie od tego czy służy do tego sprzęt będący własnością Jedność / DAP.

**Zastrzeżone i poufne informacje.** Wszystkie zasady obejmujące ochronę zastrzeżonych i poufnych informacji stosują się również do blogów oraz aktywności online. Przekazywanie poufnych materiałów klienta i dostawcy lub jakichkolwiek zastrzeżonych informacji bez zgody firmy lub klienta i dostawcy jest zabronione. Zastrzeżone i poufne informacje obejmują w szczególności: oprogramowanie komputerowe, nieopatentowane wynalazki, odkrycia oraz udoskonalenia, informacje marketingowe, produkcyjne, informacje dotyczące różnego rodzaju badań i analiz, zmian organizacyjnych, planów biznesowych, polityki firmy, prognoz sprzedaży, dane dotyczące pracowników, ceny, niedostępne publicznie dane finansowe, listy obecnych i potencjalnych klientów i dostawców oraz informacje na temat klientów, dostawców lub ich pracowników, informacje dotyczące zakupu istotnego wyposażenia firmy lub nieruchomości.

|                                                                                                                                            |                    |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------|
| <br><b>Polityka bezpieczeństwa i poufności informacji</b> | Strona/Stron       | 10/16      |
|                                                                                                                                            | Wydanie            | 1          |
| <b>Dokument stworzył: Marek Garbacz</b><br><b>Zaakceptował: Adam Ogonowski</b>                                                             | Data obowiązywania | 24.06.2024 |
|                                                                                                                                            |                    |            |

### **Własność intelektualna firmy.**

Zabronione jest używanie narzędzi dostępnych w mediach społecznościowych do kopiowania, publikowania lub przesyłania jakichkolwiek materiałów chronionych prawem autorskim, instrukcji, procedur, zdjęć, filmów, dokumentacji technicznych maszyn, urządzeń, planów budynków, publikacji w formie cyfrowej włączając w to znaki ochrony własności intelektualnej, logo oraz materiały związane z marką firmy Jedność / DAP .

### **Pracownicy nie mogą reprezentować firmy.**

Angażując się w działania w mediach społecznościowych, pracownicy nie mogą występować w imieniu firmy, reprezentować stanowiska Jedność / DAP ani poglądu osób czy organizacji stowarzyszonych lub współpracujących biznesowo z Jedność / DAP. Jeśli tematem stworzonej przez pracownika treści jest firma, pracownik powinien jasno doprecyzować, że jest pracownikiem firmy oraz że nie reprezentuje w swoich poglądach firmy. Pracownik prowadząc blog lub w inny sposób publikując treści online powiązane ze swoją pracą czy też tematycznie związane z firmą, powinien wyjaśnić, że nie wypowiada się w imieniu firmy. Najlepiej jeśli zawrze zastrzeżenie takie, jak: „wypowiedzi na tej stronie są mojego autorstwa i nie odzwierciedlają poglądów Wydawnictwa Jedność / Drukarni DAP

Niemniej jednak jeśli pracownik zdecyduje się na publikowanie nieprawidłowości lub krytyki, powinien unikać wypowiedzi, które mogłyby być postrzegane jako złośliwe, obsceniczne, grożące lub zastraszające albo dyskredytujące klientów, pracowników czy dostawców. Przykłady takiego postępowania mogą obejmować obraźliwe wypowiedzi, celowo godzące w czyjąś reputację lub stwierdzenia, które mogą przyczynić się do tworzenia środowiska wrogo nastawionego wobec rasy, płci, niepełnosprawności, religii albo innego statusu chronionego prawem lub niezgodnego z zasadami panującymi w firmie. Do reprezentowania firmy w kreślonym zakresie są uprawnione jedynie osoby posiadające pełnomocnictwo nadane przez dyr. Ks. Leszka Skorupę. Pełnomocnictwo to zawiera szczegółowo zakres a załącznik do niego listę osób uprawnionych do reprezentowania firmy.

|                                                                                                                                            |                    |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------|
| <br><b>Polityka bezpieczeństwa i poufności informacji</b> | Strona/Stron       | 11/16      |
|                                                                                                                                            | Wydanie            | 1          |
| <b>Dokument stworzył: Marek Garbacz</b><br><b>Zaakceptował: Adam Ogonowski</b>                                                             | Data obowiązywania | 24.06.2024 |
|                                                                                                                                            |                    |            |

## **Zdjęcia i filmy.**

Pracownicy nie mogą publikować w serwisach społecznościowych zdjęć i filmów przedstawiających innych pracowników, klientów lub dostawców bez zgody tych osób. Pracownicy nie mogą publikować zdjęć osób zaangażowanych w działalność przedsiębiorstwa, zdjęć zrobionych podczas spotkań firmowych ani przedstawiających obiekty, sprzęt lub produkty klientów i dostawców bez wyraźnej zgody firmy.

## **Sprzedaż lub reklama produktów i usług firmy.**

Pracownicy nie powinni umieszczać w mediach społecznościowych żadnych reklam, zdjęć lub filmów informujących o produktach firmy i nie mogą angażować się w ten sposób w sprzedaż produktów i usług firmy. Wyjątkiem mogą być pracownicy, którzy zostali wyraźnie upoważnieni do reprezentowania firmy w serwisach społecznościowych.

## **Publikowanie poza @jednosc.com.pl, @dap.pl**

W ramach realizacji zleczanych zadań nie wolno pracownikom udostępniać treści firmowych osobom spoza domeny @jednosc.com.pl, @dap.pl z wyjątkiem sytuacji, gdy jest to wyraźnie wymagane i zezwolone.

## **Zastrzeżone i poufne informacje klientów i dostawców.**

Przekazywanie poufnych danych firmy lub klientów i dostawców poprzez media i portale społecznościowe jest surowo zabronione, nawet gdyby te informacje były widoczne poprzez @jednosc.com.pl, @dap.pl lub inne domeny firmowe.

## **Polityka ma zastosowanie pomimo szerszych możliwości technicznych.**

Nawet jeśli serwisy społecznościowe, dostarczone przez Jedność / DAP, dają pracownikom większe możliwości techniczne niż te, które omawia niniejsza polityka, to pracownicy są zobowiązani do przestrzegania zasad wymienionych w tej polityce oraz innych mających zastosowanie firmowych zasad.

|                                                                                                                                            |                    |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------|
| <br><b>Polityka bezpieczeństwa i poufności informacji</b> | Strona/Stron       | 12/16      |
|                                                                                                                                            | Wydanie            | 1          |
| <b>Dokument stworzył: Marek Garbacz</b><br><b>Zaakceptował: Adam Ogonowski</b>                                                             | Data obowiązywania | 24.06.2024 |
|                                                                                                                                            |                    |            |

## Kontrola pracodawcy

Firma zastrzega sobie prawo do korzystania z narzędzi do zarządzania treścią, w celu monitorowania, przeglądania lub blokowania zawartości serwisów społecznościowych, które naruszają tą lub jakiegokolwiek inną politykę firmy. Dotyczy to zarówno serwisów społecznościowych dostarczanych przez firmę, jak i pozostałych. Dostęp poszczególnych użytkowników do serwisów społecznościowych jest monitorowany i kontrolowany przez upoważnionego pracownika w obszarze IT. Wniosek o dostęp do portali społecznościowych musi zostać uzasadniony biznesowo oraz poparty zgodą menedżera danego działu.

Ostrzega się pracowników, że zasady prywatności nie mają zastosowania podczas korzystania z internetu oraz mediów społecznościowych. Niechronione wypowiedzi mogą być przeglądane przez wszystkie osoby, w tym osoby z firmy. Jedność / DAP zastrzega sobie prawo do monitorowania komentarzy oraz dyskusji na temat firmy, jej pracowników, klientów oraz branży (w tym produktów i konkurentów), udostępnionych w mediach społecznościowych przez każdego, czyli pracowników oraz osoby spoza firmy.

Jedność / DAP może, według własnego uznania, wykorzystywać narzędzia i oprogramowanie w celu monitorowania mediów społecznościowych. Ostrzega się, iż pracownicy używający sprzętu firmowego w dowolnym celu, w tym do uprawnionego korzystania z mediów społecznościowych, nie mogą oczekiwać respektowania zasady prywatności.

## Zgłoszenie naruszenia polityki

Jedność / DAP zachęca pracowników do zgłaszania wszelkich rzeczywistych, możliwych czy zauważanych naruszeń niniejszej polityki. Wszelkie naruszenia powinny być zgłaszane do przełożonych, menedżerów, Działu ds. Personalnych lub za pośrednictwem infolinii ds. etyki. Każdy pracownik, który zastosuje środki odwetowe wobec innego pracownika, zgłaszającego ewentualne odstępstwa od tej polityki lub wobec pracownika pomagającego w dochodzeniu, może podlegać postępowaniu dyscyplinarnemu, z rozwiązaniem umowy włącznie.

## Sankcje dyscyplinarne oraz konsekwencje nieprzestrzegania polityki

|                                                                                                                                            |                    |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------|
| <br><b>Polityka bezpieczeństwa i poufności informacji</b> | Strona/Stron       | 13/16      |
|                                                                                                                                            | Wydanie            | 1          |
| <b>Dokument stworzył: Marek Garbacz</b><br><b>Zaakceptował: Adam Ogonowski</b>                                                             | Data obowiązywania | 24.06.2024 |
|                                                                                                                                            |                    |            |

Jedność / DAP będzie wnikliwie badać i reagować na wszelkie doniesienia o łamaniu zasad tej polityki oraz polityk z nią powiązanych. Naruszenie polityki użytkowania mediów społecznościowych będzie skutkowało działaniami dyscyplinującymi a nawet zwolnieniem. Decyzja o sankcjach lub wypowiedzeniu umowy o pracę uzależniona będzie od dotychczasowego przebiegu pracy danego pracownika w firmie oraz od rodzaju i skutków naruszenia tej polityki.

Jedność / DAP zastrzega sobie prawo do wszczęcia postępowania sądowego przeciwko pracownikom zaangażowanym w zabronione i niezgodne z prawem postępowanie. Ponadto, w zależności od charakteru działania, pracownicy, którzy naruszają zasady tej polityki i/lub prawa mogą podlegać cywilnym i/lub karnym sankcjom.

### **Nieingerowanie**

Poniższa polityka nie stoi w sprzeczności z przepisami prawa pracy, w szczególności z przepisami Kodeksu Pracy oraz innymi obowiązującymi regulacjami prawnymi.

### **Własność intelektualna i bezpieczeństwo informacji**

Szanujemy prawa własności intelektualnej, w związku z czym przekazywanie technologii lub know-how powinno odbywać się w sposób zapewniający ochronę praw własności intelektualnej. Informacje o klientach należy zabezpieczać zgodnie z obowiązującym prawem i przepisami

### **Ochrona informacji osób trzecich i prywatności klienta**

Dążymy do odpowiedniej ochrony prywatności danych osobowych wszystkich osób, z którymi prowadzimy interesy, w tym naszych dostawców, klientów, konsumentów i pracowników. Przestrzegamy przepisów w zakresie prywatności i bezpieczeństwa informacji oraz wymogów regulacyjnych podczas zbierania, przechowywania, przetwarzania, przekazywania i udostępniania informacji.

|                                                                                                                                            |                    |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------|
| <br><b>Polityka bezpieczeństwa i poufności informacji</b> | Strona/Stron       | 14/16      |
|                                                                                                                                            | Wydanie            | 1          |
| <b>Dokument stworzył: Marek Garbacz</b><br><b>Zaakceptował: Adam Ogonowski</b>                                                             | Data obowiązywania | 24.06.2024 |
|                                                                                                                                            |                    |            |

## Sprzeniewierzenie zasobów

Będziemy korzystać z zasobów naszej grupy wyłącznie zgodnie z ich przeznaczeniem biznesowym i będziemy je chronić przed utratą, uszkodzeniem, kradzieżą, marnotrawstwem lub innym niewłaściwym wykorzystaniem. W celu ochrony naszych zasobów, należy wdrożyć odpowiednie środki kontrolne pozwalające zapobiegać nieuczciwym działaniom (np. oszustwom, defraudacji, kradzieży, przywłaszczeniu, uchylaniu się od płacenia podatków lub praniu brudnych pieniędzy). W razie wykrycia lub uzyskania wiedzy o sprzeniewierzeniu zasobów, niezależnie od tego, czy jest ono wymierzone przeciw nam, czy przeciw naszym klientom, dostawcom lub partnerom, należy zgłosić to przełożonemu lub dyrektorowi zarządzającemu.

### Przykłady:

#### Zasoby spółki obejmują:

- mienie fizyczne, np. lokale, wyposażenie biurowe, komputery, telefony, fundusze firmowe, Kodeks etycznej działalności gospodarczej | 11
- informacje poufne i zastrzeżone, np. listy klientów, dane na temat szans sprzedażowych, biznesplany, dokumentacja umowna oraz zamówienie
- własność intelektualna, w tym patenty, znaki towarowe, prawa autorskie i nazwy domen.

Zarządzenie wchodzi w życie z dniem 01.07.2024 r. jako załącznik nr. xxx do Regulaminu Pracy Wydawnictwa Jedność.

Należy pamiętać iż KP reguluje obowiązki pracownika jako dwa rodzaje odpowiedzialności:

Materialnej pracownika względem pracodawcy: odpowiedzialność tzw. ogólną za szkodę wyrządzoną pracodawcy, z winy umyślnej bądź nieumyślnej (art. 114-122 k.p.) oraz odpowiedzialność za mienie powierzone z obowiązkiem zwrotu albo wyliczenia (art. 124-127 k.p.).

|                                                                                                                                            |                    |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------|
| <br><b>Polityka bezpieczeństwa i poufności informacji</b> | Strona/Stron       | 15/16      |
|                                                                                                                                            | Wydanie            | 1          |
| <b>Dokument stworzył: Marek Garbacz</b><br><b>Zaakceptował: Adam Ogonowski</b>                                                             | Data obowiązywania | 24.06.2024 |
|                                                                                                                                            |                    |            |

Odpowiedzialność materialna pracownika, tzw. ogólna za szkodę wyrządzoną pracodawcy wskutek niewykonania lub nienależytego wykonania obowiązków, jest odpowiedzialnością majątkową pracownika. Pracownik ponosi odpowiedzialność na podstawie art. 114–122 k.p. wówczas, gdy pracodawca udowodni okoliczności uzasadniające tę odpowiedzialność.

Okoliczności te to, po pierwsze bezprawność, czyli niewykonanie lub nienależyte wykonanie obowiązków pracowniczych, które ma miejsce w sytuacji, gdy pracownik działa sprzecznie z ciążącym na nim obowiązkiem lub gdy nie podejmuje się działań, mimo że jest do nich zobowiązany;

Po drugie winę pracownika, która może być winą umyślną tj., gdy pracownik naruszając obowiązek pracowniczy chce wyrządzić pracodawcy szkodę bądź poprzez naruszenie obowiązku pracowniczego godzi się na wyrządzenie takiej szkody lub może mieć postać winy nieumyślnej, tj. kiedy pracownik, mimo że ją przewiduje, nie ma zamiaru wyrządzenia pracodawcy szkody, jednakże całkowicie nieuzasadnienie przypuszcza, iż jej nie wyrządzi bądź w ogóle jej nie przewiduje, mimo że mógł ją przewidzieć,

Po trzecie wysokość rzeczywistej szkody, która wynika z wyrządzenia szkody w majątku pracodawcy. Może m.in. polegać na zmniejszeniu aktywów pracodawcy (np. zniszczenie towaru) bądź na zwiększeniu jego pasywów (np. wypłata odszkodowania klientowi z powodu opóźnienia w dostawie towaru z winy pracownika). W tym miejscu warto podkreślić, iż w przypadku zniszczenia się rzeczy związanej z normalnym i zwyczajowo przyjętym użytkowaniem, nie mamy do czynienia ze szkodą pracodawcy;

Po czwarte naturalny związek przyczynowy między szkodą a zachowaniem pracownika. Zgodnie z orzeczeniem Sądu Najwyższego pracownik, na podstawie art. 114 k.p. ponosi odpowiedzialność za szkodę poniesioną przez pracodawcę tylko w razie zawinionego niewykonania obowiązków pracowniczych, pozostającego w związku przyczynowym ze szkodą (wyrok SN z dnia 11 maja 1977 r., IV PR 109/77)

|                                                                                                                                            |                    |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------|
| <br><b>Polityka bezpieczeństwa i poufności informacji</b> | Strona/Stron       | 16/16      |
|                                                                                                                                            | Wydanie            | 1          |
| <b>Dokument stworzył: Marek Garbacz</b><br><b>Zaakceptował: Adam Ogonowski</b>                                                             | Data obowiązywania | 24.06.2024 |
|                                                                                                                                            |                    |            |

---

**KONIEC**