



Fundusze Europejskie
dla Nowoczesnej Gospodarki



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



REGULAMIN BEZPIECZEŃSTWA INFORMACJI PRZETWARZANYCH W SYSTEMIE INFORMATYCZNYM DIG.IT

Projekt niekonkurencyjny grantowy „Dig.IT. Transformacja cyfrowa”

program Fundusze Europejskie dla Nowoczesnej Gospodarki 2021-2027

Działanie 2.21 Dig.IT Transformacja cyfrowa

§ 1.

POSTANOWIENIA OGÓLNE

1. Niniejszy „Regulamin Bezpieczeństwa Informacji przetwarzanych w Systemie Informatycznym Dig.IT” (dalej określany jako „Regulamin”) określa prawa i obowiązki Użytkowników Systemu Informatycznego Dig.IT w zakresie generowania, składania i obsługi Wniosków o przyznanie grantu, zasady, zakres i warunki korzystania przez Użytkowników z przedmiotowego Systemu oraz zasady bezpieczeństwa informacji, w tym ochrony danych osobowych Użytkowników Systemu przetwarzanych w tym Systemie.
2. Ilekroć w Regulaminie jest mowa o:
 - a) **ARP S.A.** – należy przez to rozumieć Agencję Rozwoju Przemysłu S.A z siedzibą przy ul. Nowy Świat 6/12, 00-400 Warszawa;
 - b) **Administratorze Systemu** – należy przez to rozumieć ARP S.A.;
 - c) **Incydencie** – należy przez to rozumieć pojedyncze zdarzenie lub serię niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji lub zmniejszeniem poziomu dostępności usług w Systemie, które stwarzają znaczne prawdopodobieństwo zakłócenia dostępności lub działania Systemu, lub zagrażają bezpieczeństwu informacji, w tym danych osobowych przetwarzanych w Systemie;
 - d) **Instrukcji Użytkownika** – należy przez to rozumieć „Instrukcję użytkownika Systemu Informatycznego Dig.IT”, dostępną na Stronie Internetowej Projektu Dig.IT lub za pośrednictwem Systemu;
 - e) **Hasła** - należy przez to rozumieć unikalne w ramach Systemu hasło dla Konta Użytkownika utworzone zgodnie z zasadami określonymi w niniejszym dokumencie;
 - f) **Konkursie** – należy przez to rozumieć nabór organizowany przez ARP S.A. w ramach Projektu Dig.IT, w ramach którego następuje składanie Wniosków o przyznanie grantu przez Wnioskodawców, a następnie dokonywana jest ocena na podstawie regulaminu konkursu;
 - g) **Koncie** – należy przez to rozumieć dedykowaną Użytkownikowi przestrzeń cyfrową Systemu dostępną za pośrednictwem Loginu i zabezpieczoną Hasłem. Konto służy do identyfikacji Użytkownika i zapewnia mu bezpieczny dostęp do danych, plików oraz funkcji Systemu. Posiadanie Konta pozwala na spersonalizowane korzystanie z Systemu, w związku z czym Konto jest przypisane do jednego Użytkownika i nie może zostać przeniesione na innego Użytkownika;
 - h) **Loginie** – należy przez to rozumieć unikalną w ramach Systemu nazwę Użytkownika utworzoną zgodnie z zadaniami określonymi w niniejszym dokumencie;
 - i) **Operatorze Systemu** – należy przez to rozumieć spółkę ARP Informatyka Sp. z o.o. z siedzibą przy ul. Nowy Świat 6/12, 00-400 Warszawa, która w imieniu Administratora Systemu zapewnia obsługę informatyczną Systemu;
 - j) **Podatności** – należy przez to rozumieć lukę (słabość) aktywu lub grupy aktywów, która może być wykorzystana przez co najmniej jedno zagrożenie, rozumiane jako potencjalna przyczyna niepożądanego Incydentu, który może wywołać szkodę w Systemie;

- k) **Projekcie Dig.IT** – należy przez to rozumieć realizowany przez ARP S.A. projekt niekonkurencyjny grantowy pt. „Dig.IT. Transformacja cyfrowa”, współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach programu Fundusze Europejskie dla Nowoczesnej Gospodarki na lata 2021-2027;
 - l) **Przetwarzaniu** – należy przez to rozumieć operacje wykonywane w Systemie na danych, w tym danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, np. zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
 - m) **Strona Internetowa Projektu Dig.IT** – należy przez to rozumieć stronę internetową www.digit.arp.pl;
 - n) **Systemie** lub **Systemie Informatycznym Dig.IT** lub **SI Dig.IT** – należy przez to rozumieć narzędzie informatyczne przeznaczone do składania Wniosków w ramach Projektu Dig.IT, umożliwiające m.in.: zamieszczanie przez ARP S.A. informacji dotyczących Konkursu oraz składanie Wniosków przez Wnioskodawców.
 - o) **Użytkownika** – należy przez to rozumieć osobę mającą Konto w Systemie, reprezentującą Wnioskodawcę lub Operatora Systemu uprawnionych do wykonywania (odpowiednio) w imieniu Wnioskodawcy lub Administratora Systemu czynności wynikających z funkcjonalności Systemu. System przewiduje następujące typy Użytkowników:
 - **Użytkownik Zewnętrzny** – należy przez to rozumieć Użytkownika działającego w imieniu Wnioskodawcy;
 - **Użytkownika Specjalny** – należy przez to rozumieć Użytkownika ze strony Operatora Systemu reprezentującego Administratora Systemu tj. użytkownika Systemu o specjalnych uprawnieniach, które pozwalają na m.in. na zarządzanie Systemem;
 - p) **Wniosku** – Wniosek o powierzenie grantu (WOPG) na Transformację cyfrową wraz z załącznikami, składany przez Wnioskodawcę, w celu wzięcia udziału w Konkursie ogłoszonym przez ARP S.A. i uzyskania Grantu;
 - q) **Wnioskodawcy** – należy przez to rozumieć podmiot, który złożył Wniosek do ARP S.A. w ramach ogłoszonego Konkursu;
 - r) **Zdarzeniu związanym z bezpieczeństwem informacji** – należy przez to rozumieć stan Systemu, usługi lub sieci, wskazujący na możliwe naruszenie Regulaminu, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.
- 3. System jest utrzymywany i nadzorowany przez ARP S.A. oraz stanowi jej wyłączną własność.
 - 4. System dostępny jest pod adresem: wnioski.digit.arp.pl
 - 5. Niniejszy Regulamin ma zastosowanie wobec wszystkich Użytkowników Systemu.
 - 6. Niniejszy Regulamin określa:
 - a) warunki korzystania z Systemu;
 - b) zasady rejestracji i zarządzania Kontami Użytkowników Systemu;

- c) uprawnienia i obowiązki Użytkownika Systemu;
- d) zasady dostępu i pracy w Systemie;
- e) zasady bezpieczeństwa korzystania z Systemu;
- f) zasady zgłaszania Incydentów i Podatności oraz innych potencjalnych błędów w działaniu Systemu;
- g) zasady przetwarzania danych osobowych Użytkowników Systemu;
- h) zasady prowadzenia komunikacji zastępczej w przypadku niedostępności Systemu.

§ 2.

WARUNKI KORZYSTANIA Z SYSTEMU

1. Dostęp do Systemu jest dobrowolny i bezpłatny.
2. System dostępny jest w trybie ciągłym przez 24 godziny na dobę.
3. W związku z prowadzeniem prac konserwacyjnych w Systemie lub modyfikacją funkcjonalności Systemu lub ze względów bezpieczeństwa lub z innych niezależnych przyczyn Administrator Systemu ma prawo czasowo zawiesić dostęp Użytkowników do Systemu w okresie wskazanym w ust. 2, na okres niezbędny do przeprowadzenia planowanych prac lub wyeliminowania niepożądanych zdarzeń. O przerwach w dostępności Systemu Administrator Systemu poinformuje każdorazowo na Stronie Internetowej Projektu Dig.IT.
4. Korzystanie z Systemu jest możliwe tylko na urządzeniach stacjonarnych lub laptopach z odpowiednim oprogramowaniem i konfiguracją sprzętową (komputer).
5. System nie wspiera dostępu ani funkcjonalności na urządzeniach mobilnych, dlatego próby korzystania z systemu na tego typu urządzeniach mogą skutkować błędami lub brakiem dostępu.
6. Do prawidłowego i bezpiecznego korzystania z Systemu niezbędne jest:
 - a) połączenie z siecią Internet;
 - b) użycie przeglądarki internetowej w aktualnej, stabilnej wersji, objętej wsparciem bezpieczeństwa przez producenta np. Google Chrome, Mozilla Firefox, Microsoft Edge, Safari lub inna równoważna.
7. Komputer Użytkownika powinien posiadać system operacyjny w aktualnej, stabilnej wersji, objętej wsparciem bezpieczeństwa przez producenta. Wszelkie aktualizacje krytyczne powinny być instalowane niezwłocznie.
8. Komputer Użytkownika powinien posiadać oprogramowanie antywirusowe, którego sygnatury wirusów powinny być aktualizowane nie rzadziej niż raz na tydzień. Oprogramowanie antywirusowe powinno być stale aktywne.
9. Komputer Użytkownika powinien być chroniony zaporą sieciową (firewall).
10. Użytkownik jest zobowiązany do stałego monitorowania komunikatów pochodzących z oprogramowania antywirusowego i zapory sieciowej oraz reagowania na nie.
11. Komputer Użytkownika powinien posiadać dostęp do przeglądarki internetowej w aktualnej, stabilnej wersji, objętej wsparciem bezpieczeństwa przez producenta.

12. Sprzęt i oprogramowanie komputera Użytkownika, na którym uruchamiany jest System, powinny być regularnie aktualizowane, zgodnie z wytycznymi producentów. W szczególności dotyczy to systemu operacyjnego oraz przeglądarki internetowej.
13. Zabrania się Użytkownikowi nieautoryzowanego monitorowania Systemu, w tym jego zabezpieczeń oraz podejmowania przez Użytkownika jakichkolwiek prób mających na celu naruszenie bezpieczeństwa danych przetwarzanych w Systemie, w tym prób przełamania zabezpieczeń Systemu.
14. Użytkownik jest zobowiązany do zgłaszania przypadków naruszenia bezpieczeństwa informacji lub naruszenia bezpieczeństwa danych osobowych w sposób określony w § 7 Regulaminu.
15. ARP S.A. nie ponosi odpowiedzialności za brak dostępu do Systemu z przyczyn niezależnych od ARP S.A., tj. działania siły wyższej, awarii Komputera Użytkownika, nieodstępności łącza internetowego Użytkownika lub niedozwolonej ingerencji Użytkowników lub osób trzecich, w tym również jeśli spowodowałyby one utratę danych na Kontach Użytkowników.
16. ARP S.A. nie ponosi odpowiedzialności za szkody powstałe w związku z korzystaniem z Systemu, bądź w związku z niewłaściwym działaniem Systemu spowodowanym: błędami, brakami, zakłóceniami, defektami, opóźnieniami w transmisji danych, wirusami komputerowymi, awariami łącza sieci Internet lub nieprzestrzeganiem postanowień Regulaminu przez Użytkownika.
17. W przypadku, gdy z powodów technicznych komunikacja z ARP S.A. poprzez System nie będzie możliwa, powinna ona następować za pośrednictwem komunikacji zastępczej określonej w Regulaminie Konkursu tj. poczcie elektronicznej przesyłanej z adresu e-mail wskazanego przez Użytkownika Systemu na etapie tworzenia konta w Systemie na adres e-mail określony przez ARP S.A. w Regulaminie Konkursu.

§ 3.

ZASADY REJESTRACJI I ZARZĄDZANIA KONTAMI UŻYTKOWNIKÓW SYSTEMU

1. Użytkownikiem Systemu może być osoba reprezentująca Wnioskodawcę lub Operatora Systemu, która zarejestruje Konto w Systemie.
2. Poziom uprawnień w Systemie uzależniony jest od typu Użytkownika i nadawany jest zgodnie z pełnioną w Projekcie funkcją.
3. System przewiduje następujące typy Użytkowników:
 - a) Użytkownik Zewnętrzny;
 - b) Użytkownik Specjalny.
4. Konto Użytkownika Zewnętrznego reprezentującego Wnioskodawcę rejestrowane jest na bazie formularza udostępnionego na stronie logowania Systemu.
5. Konta Użytkowników Specjalnych rejestrowane są zgodnie z zasadami obowiązującymi w ARP S.A.
6. Każdy Użytkownik może posiadać jedno Konto.
7. Podczas rejestracji Konta Użytkownika Zewnętrznego należy przestrzegać postanowień Instrukcji Użytkownika.

8. Uzyskanie dostępu do Systemu przez Użytkownika Zewnętrznego możliwe będzie po:
 - a) zapoznaniu się z niniejszym Regulaminem, jego zaakceptowaniu i zobowiązaniu się do jego przestrzegania przez cały okres użytkowania Systemu,
 - b) zapoznaniu się z Instrukcją Użytkownika, jej zaakceptowaniu i zobowiązaniu się do jej przestrzegania przez cały okres użytkowania Systemu oraz
 - c) wyrażeniu zgody na otrzymywanie drogą elektroniczną informacji dotyczących Systemu i powiadomień dotyczących statusu Wniosku na podany adres mailowy.
9. System będzie przechowywał informacje o dacie i godzinie złożenia przez Użytkownika Zewnętrznego oświadczeń, o których mowa w ust. powyżej.
10. W Systemie wykorzystano funkcjonalność wysyłania powiadomień na adres e-mail podany na etapie rejestracji konta w Systemie.
11. Użytkownik jest zobowiązany do dbania o bezpieczeństwo konta e-mailowego, o którym mowa powyżej, w szczególności do:
 - a) używania silnego hasła dostępu;
 - b) nieotwierania załączników do poczty i linków pochodzących z nieznanymi źródeł;
 - c) zachowania ostrożności podczas otwierania nieoczekiwanych załączników w korespondencji pochodzącej od znanych nadawców.
12. Aktywacja Konta w Systemie dla Użytkownika Zewnętrznego następuje po kliknięciu przez Użytkownika w link aktywacyjny przesłany na podany przez Użytkownika w procesie rejestracji adres e-mail, pod warunkiem, że Użytkownik:
 - a) zaakceptował wszelkie wymagane w Systemie zgody i Regulaminy oraz
 - b) poprawnie podał wymagane dane na etapie rejestracji Konta.
13. Użytkownik Zewnętrzny ma obowiązek aktywacji Konta w ciągu 24 godzin od momentu otrzymania linku aktywacyjnego. Konta nieaktywowane we wskazanym terminie będą usuwane w sposób automatyczny. Użytkownik Zewnętrzny, który nie aktywuje Konta we wskazanym terminie będzie musiał ponownie zarejestrować konto Użytkownika.
14. W celu korzystania z Systemu niezbędne jest uwierzytelnienie Użytkownika przy wykorzystaniu Loginu i Hasła.
15. W przypadku Użytkowników Zewnętrznych Loginem jest nazwa użytkownika zgłoszona na etapie rejestracji Konta.
16. W celu zachowania bezpieczeństwa Systemu obowiązują następujące zasady konfiguracji Hasła dostępu:
 - a) składa się z minimum 8 znaków (maksymalny rozmiar hasła wynosi 64 znaki);
 - b) zawiera wielkie i małe litery, co najmniej jedną cyfrę oraz co najmniej jeden znak specjalny;
 - c) nie używa słów ze słownika lub prostych sekwencji klawiszowych np. "qwerty", "123456";
 - d) powinno być unikalne, tj. zabronione jest użycie hasła wykorzystywanego w innych kontach lub usługach.

17. Niedozwolone jest udostępnianie Loginu i Hasła osobom trzecim.
18. Niedozwolone jest zapisywanie Loginu i Hasła w miejscach dostępnych dla osób trzecich, w tym w plikach tekstowych na komputerze lub karteczkach przy biurku.
19. W przypadku zaistnienia ryzyka nieumyślnego ujawnienia Loginu i Hasła osobie trzeciej lub wycieku danych logowania, Użytkownik ma obowiązek niezwłocznie zgłosić ten fakt i zmienić Hasło.
20. Zmiana Hasła możliwa jest za pośrednictwem funkcjonalności „Zapomniałem hasło” dostępnej z poziomu strony logowania Systemu. Po wpisaniu adresu e-mailowego do którego przypisane jest konto, należy kliknąć „Wyślij”. Wówczas System wysyła na adres mailowy Użytkownika link do aktywacji konta umożliwiający ponowne utworzenie Hasła.
21. W przypadku braku możliwości dokonania przez Użytkownika zmiany Hasła (braku działania funkcjonalności „Zapomniałem hasło”), należy powiadomić Administratora Systemu wysyłając wiadomość na adres: digit@arp.pl. Wiadomość powinna zawierać jak najbardziej szczegółowy opis sytuacji oraz w miarę możliwości, zrzuty z ekranu ilustrujące zaistniały problem.
22. Po zakończeniu pracy z Systemem Użytkownik zobowiązany jest się wylogować, by zapobiec nieautoryzowanemu dostępowi do Konta.
23. Administrator Systemu zastrzega sobie prawo do zawieszenia Konta Użytkownika, który narusza prawo lub postanowienia Regulaminu.
24. ARP S.A. może trwale zablokować Konto, jeśli Użytkownik nie zaprzestanie działań sprzecznych z prawem lub postanowieniami Regulaminu.
25. O zawieszeniu lub zablokowaniu konta Użytkownik zostaje poinformowany przez Administratora Systemu mailowo, niezwłocznie po podjęciu decyzji, podając przyczynę oraz warunki przywrócenia dostępu.
26. Użytkownik ma prawo złożyć odwołanie od decyzji o blokadzie lub zawieszeniu konta w terminie 3 dni roboczych od dnia wysyłki powiadomienia przez Administratora Systemu.
27. Odwołanie będzie rozpatrzone niezwłocznie, a w przypadku podtrzymania decyzji Użytkownik zostanie o tym poinformowany z uzasadnieniem.
28. W przypadku naruszeń szczególnie poważnych lub powtarzających się Konto może zostać trwale zablokowane przez Administratora Systemu bez możliwości przywrócenia.
29. Użytkownik ma prawo do trwałego usunięcia swojego Konta.
30. Trwałe usunięcie Konta Użytkownika odbywa się w przypadku:
 - a) Konta Użytkownika Zewnętrznego reprezentującego Wnioskodawcę jako osoba uprawniona do zarządzania Użytkownikami - zgłoszenia przesłanego przez Użytkownika Zewnętrznego na adres digit@arp.pl;
 - b) Kont Użytkowników Specjalnych reprezentujących Operatora Systemu - zgodnie z zasadami obowiązującymi w ARP S.A
31. Po akceptacji wniosku o likwidację Konta, System rozpocznie proces usuwania danych użytkownika w terminie do 10 dni roboczych, o ile nie istnieją przesłanki prawne do zachowania danych.

32. Usunięcie Konta jest nieodwracalne. Po zakończeniu procesu likwidacji użytkownik traci dostęp do wszystkich udostępnionych Użytkownikowi usług i danych w Systemie.
33. Po złożeniu pierwszej wersji Wniosku o powierzenie grantu, usunięcie Konta Użytkownika nie powoduje usunięcia danych przesłanych przez Użytkownika w Systemie oraz metadanych dotyczących Użytkownika niezbędnych do zapewnienia integralności i dostępności danych w Systemie.

Administrator Systemu zastrzega sobie prawo usunięcia Kont Użytkowników, którzy nie logowali się do systemu przez okres 24 miesięcy. O planowanym usunięciu Konta Użytkownik zostaje poinformowany przez Administratora Systemu mailowo, niezwłocznie po podjęciu decyzji, podając przyczynę oraz warunki utrzymania dostępu do Systemu.

§ 4.

UPRAWNIENIA I OBOWIĄZKI UŻYTKOWNIKA SYSTEMU

1. Użytkownik Zewnętrzny Systemu ponosi pełną odpowiedzialność za treści umieszczane przez niego w Systemie, w tym za treści znajdujące się w załączanych przez niego dokumentach (bądź stronach, których linki udostępnia w systemie, jako odsyłacze).
2. Użytkownik Zewnętrzny Systemu ponosi pełną odpowiedzialność za złamanie prawa bądź szkodę wywołaną jego działaniami w Systemie, w szczególności podaniem nieprawdziwych danych.
3. Użytkownik Zewnętrzny wprowadzający dane do Systemu zobowiązany jest w szczególności do: zapewnienia ich jakości, prawdziwości oraz zgodności ze strukturą danych oczekiwanych przez System.
4. Administrator Systemu nie ponosi odpowiedzialności za treści umieszczane w Systemie przez Użytkownika.
5. Odpowiedzialność za udostępnienie danych identyfikacyjnych Konta osobom trzecim oraz za potencjalnie negatywne konsekwencje wynikające z takiego udostępnienia spoczywa wyłącznie na Użytkowniku.
6. W przypadku stwierdzenia podania przez Użytkownika nieprawdziwych lub nieaktualnych danych podanych na etapie rejestracji Konta bądź też w przypadku zidentyfikowania działań Użytkownika niezgodnych z postanowieniami niniejszego Regulaminu lub z Instrukcją Użytkownika, Administrator Systemu może:
 - a) wezwać Użytkownika do natychmiastowego usunięcia nieprawidłowości lub
 - b) zablokować Konto Użytkownika do czasu wyjaśnienia sprawy lub
 - c) trwale zablokować Konto Użytkownika
7. ARP S.A. nie ponosi odpowiedzialności za skutki zablokowania Użytkownikowi dostępu do Konta, nawet w sytuacji trwającego naboru Wniosków, skutkującego brakiem możliwości skutecznego złożenia przez Użytkownika przedmiotowego Wniosku.
8. ARP S.A. nie ponosi odpowiedzialności za konsekwencje wynikające z działań Użytkownika niezgodnych z niniejszym Regulaminem.

§ 5.

ZASADY DOSTĘPU I PRACY W SYSTEMIE INFORMATYCZNYM DIG.IT

1. Użytkownik Systemu odpowiedzialny jest za wszystkie czynności wykonane przez siebie w Systemie pracując na własnym koncie przy użyciu Loginu i Hasła, którymi się posługuje.
2. Zabronione jest korzystanie z Systemu z użyciem danych dostępowych innego Użytkownika.
3. Rozpoczynając pracę z Systemem Użytkownik zobowiązany jest sprawdzić ogólny stan komputera oraz ocenić jakość jego pracy np. niestandardowe komunikaty itp. oraz upewnić się że system operacyjny i przeglądarka internetowa są zaktualizowane.
4. Połączenie z Systemem jest szyfrowane. Podczas logowania się do Systemu Użytkownik ma obowiązek sprawdzić, czy:
 - a) adres strony internetowej widoczny w pasku adresowym przeglądarki zaczyna się od https;
 - b) w obrębie okna przeglądarki znajduje się mała kłódka informująca zabezpieczeniu połączenia;
 - c) czy po kliknięciu na kłódkę pojawia się informacja o tym, że certyfikat został wydany dla: *wnioski.digit.arp.pl i jest on ważny.
5. Konfiguracja przeglądarki internetowej powinna mieć włączoną obsługę protokołu OCSP (Online Certificate Status Protocol), umożliwiającego przeprowadzenie weryfikacji ważności certyfikatu Systemu.
6. Użytkownik ma obowiązek korzystania z sieci Internet w sposób, który nie zagraża bezpieczeństwu Systemu.
7. W przypadku korzystania z sieci WiFi Użytkownik zobowiązany jest do korzystania z zabezpieczonych hasłem i szyfrowanych sieci WiFi. Zabronione jest korzystanie z publicznie dostępnych lub nieznanymi lub niezabezpieczonych sieci WiFi.
8. Po poprawnym zalogowaniu do Systemu Użytkownik otrzyma w przeglądarce dostęp do ekranu startowego Systemu zawierającego aktywne przyciski wyboru modułów, do których Użytkownik ma nadany dostęp.
9. Użytkownik może pracować w danej sesji wykorzystując wyłącznie jedno posiadane Konto.
10. Niedozwolone jest jednoczesne uruchamianie kilku sesji przeglądarki/przeglądarek i równoległej pracy w Systemie na więcej niż jednym posiadanym Koncie.
11. Po zakończeniu pracy w Systemie Użytkownik zobowiązany jest wylogować się Systemu przez kliknięcie w prawym górnym rogu ekranu funkcji „Wyloguj”. Nie należy kończyć pracy poprzez zamknięcie okna przeglądarki znakiem „x”;
12. W celu chwilowego zawieszenia pracy w Systemie, Użytkownik zobowiązany jest zablokować ekran komputera (zablokować pulpit lub włączyć wygaszacz ekranu zabezpieczony hasłem). Jeśli komputer Użytkownika nie pozwala na zabezpieczenie ekranu hasłem, wówczas należy bezwzględnie wylogować się z Systemu;
13. Czas trwania nieaktywnej sesji w Systemie (czas bezczynności) wynosi 15 minut. Po upływie czasu bezczynności Użytkownik zostanie automatycznie wylogowany z Systemu. Użytkownik zostanie poinformowany, poprzez odpowiedni komunikat, o zbliżającym się wygaśnięciu sesji i przyciskiem umożliwiającym jej przedłużenie.

14. W trakcie pracy z Systemem ARP S.A. gromadzi informacje o adresie IP, z którego Użytkownik uwierzytelnia się w Systemie. ARP S.A. gromadzi adresy IP wyłącznie w celu wykrywania prób naruszenia zabezpieczeń Systemu oraz prowadzenia audytu zabezpieczeń Systemu. Logując się w Systemie Użytkownik wyraża zgodę na powyższe działania.
15. Administrator Systemu zapewnia mechanizmy tworzenia kopii zapasowych (backupu) danych Użytkowników w celu zapewnienia ich bezpieczeństwa oraz ciągłości działania Systemu.
16. Kopie zapasowe obejmują dane niezbędne do prawidłowego funkcjonowania Kont Użytkowników, w tym dane osobowe, konfiguracje oraz historię aktywności.
17. Dane Użytkowników Systemu mogą być archiwizowane w celu zapewnienia ich trwałego przechowywania, zgodnie z obowiązującymi przepisami prawa oraz wymogami organizacyjnymi ARP S.A.

§ 6.

ZASADY BEZPIECZEŃSTWA KORZYSTANIA Z SYSTEMU

1. Użytkownik zobowiązuje się niniejszym traktować wszelkie informacje uzyskane w trakcie korzystania z Systemu w formie: wizualnej, ustnej, tradycyjnej lub elektronicznej, niezależnie od faktu oznaczenia poufności materiałów i informacji, jako Informacje Poufne.
2. Użytkownik zobowiązuje się:
 - a) korzystać z Informacji Poufnych tylko w zakresie w jakim jest to konieczne pracy z Systemem;
 - b) nie ujawniać Informacji Poufnych osobom i podmiotom trzecim bez uprzedniej pisemnej zgody ARP S.A.;
 - c) chronić Informacje Poufne z należytą starannością przed użyciem niezgodnym z niniejszym Regulaminem;
 - d) nie kopiować, nie powielać ani nie rozpowszechniać Informacji Poufnych;
 - e) wymieniać Informacje Poufne jedynie w ramach kanałów komunikacji nazwanych w Regulaminie;
 - f) stosować właściwe środki w celu ochrony Informacji Poufnych przed ich ujawnieniem osobom nieuprawnionym;
 - g) bezzwłocznie informować Administratora Systemu o przypadkach, gdy Informacje Poufne zostały przekazane nieupoważnionym osobom trzecim.
3. Pracując z Systemem Użytkownik zobowiązany jest do zachowania bezpieczeństwa tego procesu. Podczas pracy Użytkownicy są zobowiązani w szczególności do stosowania następujących środków ochrony:
 - a) ustawienia ekranów monitorów w sposób uniemożliwiający osobom postronnym wgląd lub spisanie albo sfotografowanie informacji aktualnie wyświetlanej na ekranie monitora;
 - b) ustawienie komputerów w sposób utrudniający dostęp do portów zewnętrznych lub przynajmniej dostęp do portów zewnętrznych był pod kontrolą wizualną Użytkownika;
 - c) nie udostępniać komputera osobom trzecim;

4. W celu zapobieżenia nieautoryzowanemu dostępowi do Systemu Użytkownik:
 - a) nie może przechowywać Loginu i hasła do Systemu w miejscach dostępnych dla osób nieupoważnionych, np. w plikach, na kartkach papieru i w innych miejscach potencjalnie dostępnych dla osób trzecich;
 - b) nie może ujawniać danych służących do logowania do Systemu innym osobom. W szczególności hasła nie powinny być przekazywane/przesyłane za pomocą środków komunikacji elektronicznej tj. telefon, e-mail, fax itp.
5. Informacje Poufne w powyższym rozumieniu nie obejmują informacji które są powszechnie znane lub zostały podane do publicznej wiadomości bez naruszenia postanowień niniejszego Regulaminu;
6. ARP S.A. może ujawniać Informacje Poufne w granicach wymaganych przez prawo, w szczególności gdy Informacje Poufne zostaną ujawnione upoważnionym organom zgodnie z obowiązującymi przepisami prawa, orzeczeniem właściwego sądu lub decyzją właściwego organu administracji lub instytucji nadzorujących, rozliczających lub kontrolujących oraz gdy taka konieczność nastąpi w związku z ochroną praw obu lub poszczególnych Stron niniejszej Umowy. W każdym przypadku, takie ujawnienie Informacji Poufnych nastąpi jedynie w takim zakresie, w jakim jest ono niezbędne w celu zadośćuczynienia bezwzględnie obowiązującym przepisom prawa, orzeczeniu sądu lub decyzji organu administracji lub instytucji nadzorujących, rozliczających lub kontrolujących.
7. Informacje odnośnie zasad poufności informacji przetwarzanych w Systemie w ramach poszczególnych konkursów i grantów określa dokumentacja konkursowa publikowana na stronie www.digit.arp.pl

§ 7.

ZGŁASZANIE ZAGROZEŃ BEZPIECZEŃSTWA

1. Użytkownik jest zobowiązany do niezwłocznego powiadomienia ARP S.A. o:
 - a) zauważeniu Podatności,
 - b) podejrzeniu wystąpienia Incydentu,
 - c) zdarzeniu związanym z bezpieczeństwem informacji;
 - d) zauważeniu, że stan sprzętu komputerowego, zawartość zbioru danych osobowych w Systemie, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie bezpieczeństwa danych osobowych przetwarzanych w Systemie.
3. Powiadomienie, o którym mowa w ust. 1 należy przekazać do ARP S.A., wysyłając e-mail na adres: digit@arp.pl
4. W przypadku naruszenia lub podejrzenie naruszenia bezpieczeństwa danych osobowych, informacje należy zgłosić na adres: iod@arp.pl
5. Powiadomienie, o którym mowa w ust. 1 powinno zawierać:
 - a) dane kontaktowe Użytkownika dokonującego zgłoszenia,

- b) datę i godzinę wystąpienia Podatności, Zdarzenia związanego z bezpieczeństwem informacji, ochroną danych osobowych lub Incydentu,
 - c) opis Podatności, Zdarzenia związanego z bezpieczeństwem informacji, ochrony danych osobowych, Incydentu lub błędu,
 - d) nazwę i wersję używanej przeglądarki,
 - e) jeśli będzie to możliwe, zrzut ekranu lub nagranie video obrazujące opisaną sytuację.
6. Powiadomienia, o których mowa w ust. 3 i 4 obsługiwane są zgodnie z regulacjami wewnętrznymi ARP S.A.

§ 8.

PRZETWARZANIE DANYCH OSOBOWYCH

1. Administratorem danych osobowych Użytkownika Systemu, w rozumieniu przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, jest Agencja Rozwoju Przemysłu S.A. z siedzibą w Warszawie, ul Nowy świat 6/12, 00- 400 Warszawa.
2. ARP S.A. wyznaczyła inspektora ochrony danych, o którym mowa w art. 37-39 RODO. Dane kontaktowe inspektora ochrony danych w ARP: iod@arp.pl.
3. Podanie danych wymaganych do założenia Konta Użytkownika jest dobrowolne ale wymagane dla realizacji czynności określonych w ramach Projektu Dig.IT.
4. Dane osobowe Użytkownika będą przetwarzane w celu:
 - a) założenia konta Użytkownika i korzystania z Systemu – dane zawarte w formularzu rejestracyjnym;
 - b) identyfikacji podmiotu, który reprezentowany jest przez Użytkownika – w zakresie nazwy Wnioskodawcy;
 - c) komunikacji za pośrednictwem kanałów elektronicznych – adres e-mail, numer telefonu;
 - d) zapewnienia bezpieczeństwa Systemu - wszelkie dane osobowe Użytkownika i jego aktywności w Systemie;
 - e) zabezpieczenia i ochrony przed roszczeniami - wszelkie dane osobowe mogące dotyczyć roszczeń.
5. Dane osobowe Użytkownika przetwarzane w Systemie mogą być przekazywane następującym kategoriom odbiorców danych: organom władzy publicznej oraz podmiotom wykonującym zadania publiczne lub działającym na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z przepisów prawa, podmiotom świadczącym usługi niezbędne do realizacji przez ARP zadań, w tym: firmom badawczym realizującym na zlecenie Instytucji Zarządzającej FENG lub beneficjenta badania ewaluacyjne oraz specjalistycznym firmom realizującym na zlecenie Instytucji Zarządzającej FENG lub beneficjenta kontrole oraz audyty w zakresie zgodności przetwarzania powierzonych do przetwarzania danych osobowych z RODO. Dane te mogą być

- także przekazywane partnerom IT, podmiotom realizującym wsparcie techniczne lub organizacyjne, w szczególności Operatorowi Systemu.
6. Przetwarzanie danych osobowych jest zgodne z prawem i spełnia warunki, o których w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679. Dane są przetwarzane wyłącznie w celu:
 - a) Art. 6 ust. 1 lit (b) — akceptacja niniejszego Regulaminu jest tożsama z wyrażeniem zgody na korzystanie z Systemu;
 - b) Art. 6 ust. 1 lit (a) – wyrażonej zgody, przez którą rozumie się zaznaczenie checkboxa w wyniku czego w zostanie zidentyfikowany Użytkownik;
 - c) c) Art. 6 ust. 1 lit (f) - do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora Systemu – m.in. zapewnienia funkcjonalności Systemu, komunikowania się z Użytkownikiem, zapewnieniem bezpieczeństwa Systemu oraz zabezpieczenia i ochrony przed roszczeniami.
 7. Dane osobowe Użytkownika przetwarzane będą przez czas korzystania z Systemu lub prowadzenia korespondencji z Użytkownikiem. Okres przetwarzania danych osobowych może być przedłużony do czasu przedawnienia roszczeń związanych z celami w jakich zostały zebrane
 8. Przysługujące Użytkownikowi prawa w stosunku do ARP S.A. to: żądanie dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, sprzeciwu wobec przetwarzania a także prawo do przenoszenia danych. W sprawie realizacji praw można kontaktować się z inspektorem ochrony danych pod adresem mailowym wskazanym w pkt 2 powyżej.
 9. Użytkownikowi przysługuje prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych w wypadku uznania, że administrator danych osobowych naruszył przepisy o ochronie danych osobowych, w związku z przetwarzaniem przez administratora danych osobowych wprowadzonych do Systemu przez Użytkownika.
 10. Dane osobowe nie będą przekazywane do państwa trzeciego.
 11. Dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
 12. Informacje odnośnie zasad przetwarzania danych osobowych przetwarzanych w Systemie w ramach poszczególnych konkursów i grantów określa dokumentacja publikowana na Stronie Internetowej Projektu Dig.IT.

§ 9.

ZASADY PROWADZENIA KOMUNIKACJI ZASTĘPCZEJ

1. W przypadku czasowej niedostępności Systemu komunikacja pomiędzy ARP S.A. a Wnioskodawcą odbywa się za pośrednictwem poczty elektronicznej w formie wiadomości e-mail (komunikacja zastępcza).
2. Komunikacja z wykorzystaniem kanału komunikacji zastępczej prowadzona jest na zasadach określonych w Regulaminie Konkursu.

3. Dokumentacja przekazywana za pośrednictwem komunikacji zastępczej musi zostać zabezpieczona poprzez spakowanie do pliku archiwum w formacie 7.z i zabezpieczenie hasłem. Szczegółowa instrukcja prawidłowego przygotowania i zabezpieczenia dokumentów hasłem przesyłanych w ramach kanału komunikacji zastępczej znajduje się w Instrukcji Użytkownika.
4. Dokumentacja przesyłana za pośrednictwem kanału komunikacji zastępczej musi zostać dołączona do Systemu niezwłocznie po przywróceniu dostępności Systemu. Szczegółowa instrukcja prawidłowego dołączenia tego typu dokumentacji do Systemu znajduje się w Instrukcji Użytkownika.

§ 10.

POSTANOWIENIA KOŃCOWE

1. ARP S.A. zastrzega sobie możliwość zmiany Regulaminu lub jakiegokolwiek dokumentu określającego warunki korzystania z Systemu.
2. Zmiany Regulaminu obowiązują od daty wskazanej w informacji o zmianach.
3. W sprawach nieuregulowanych w Regulaminie mają zastosowanie przepisy powszechnie obowiązującego prawa.
4. Ewentualne spory mogące powstać w związku ze stosowaniem Regulaminu rozstrzygane będą przez sąd powszechny właściwy dla siedziby ARP S.A.
5. Użytkownicy zobowiązani są do bieżącego zapoznawania się ze zmianami Regulaminu.