**Załącznik nr 8**

**Wyciąg z zasad przetwarzania danych osobowych w ……………** *(nazwa podmiotu/ów prowadzącego inkubator)*

* Każda upoważniona do przetwarzania danych osobowych osoba zobowiązana jest do ochrony danych osobowych przed dostępem do nich osób nieuprawnionych, niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.
* Osoby przetwarzające dane osobowe zobowiązane są do zabezpieczenia materiałów zawierających dane osobowe w sposób uniemożliwiający nieuprawniony dostęp do danych osobowych osobom nieupoważnionym do ich przetwarzania, nieuprawnione ujawnienie danych, nieautoryzowany dostęp, niedozwolone: powielenie, modyfikację, zniszczenie, utratę, nieprawidłowe wykorzystanie lub kradzież.
* W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej osoby upoważnione zobowiązane są do niepozostawiania materiałów zawierających dane osobowe w miejscach umożliwiających fizyczny dostęp do nich osobom nieuprawnionym.
* Po zakończeniu pracy lub podczas czasowej przerwy w pracy, jeżeli dostęp do pomieszczenia mają osoby nieposiadające upoważnienia do przetwarzania tych danych, materiały zawierające dane osobowe winny być przechowywane w szafach zamykanych na klucz (tzw. zasada czystego biurka).
* Niedopuszczalne jest pozostawianie materiałów zawierających dane osobowe na biurku, regale, w niezamkniętej szafie i innych miejscach, do których mają dostęp inne osoby.
* Zakazane jest umożliwianie wstępu do pomieszczeń, w których przetwarzane są dane osobowe, osobom trzecim pozostawionym bez nadzoru.
* Kopiowanie danych osobowych może odbywać się wyłącznie przez osobę w ramach posiadanego przez nią upoważnienia do przetwarzania danych osobowych, w związku z realizacją czynności zawodowych. Kopie danych osobowych podlegają zniszczeniu niezwłocznie po realizacji celu, dla którego zostały wykonane.
* Dokonywanie wydruków, skanowanie lub kopiowanie materiałów zawierających dane osobowe odbywa się wyłącznie przy obecności pracownika przy urządzeniu. Niedozwolone jest pozostawianie urządzenia w trakcie drukowania/skanowania/kopiowania bez nadzoru, jeżeli materiały znajdujące się w urządzeniu zawierają dane osobowe.
* Każdy dokument papierowy zawierający dane osobowe sporządzony jako dokument roboczy należy najpóźniej na koniec dnia pracy zniszczyć lub zamknąć w miejscu uniemożliwiającym dostęp osób nieuprawnionych.
* Niszczenia brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe dokonuje się wyłącznie w niszczarkach lub umieszcza w kontenerach na dokumenty przeznaczone do zniszczenia przez podmiot profesjonalny.
* Pracownicy upoważnieni do przetwarzania danych osobowych nie mogą ich ujawniać zarówno w samej organizacji, jak i poza nią, w zakresie wykraczającym poza wykonywanie swoich obowiązków.
* Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza siedzibę organizacji bez związku z wykonywaniem czynności zawodowych.
* Zakazane jest udzielanie informacji dotyczących danych osobowych na podstawie prośby o takie dane w formie zapytania telefonicznego, z wyjątkiem udostępniania danych służbowych. Odstępstwa od tej zasady muszą być każdorazowo indywidualnie konsultowane z kierownictwem.
* Kopiowanie danych osobowych na przenośne nośniki informacji i sporządzanie wydruków tych danych jest zabronione, chyba że ich sporządzenie jest niezbędne do realizacji obowiązków służbowych, nośnik jest nośnikiem służbowym administratora, a osoba przetwarzająca dane w taki sposób uzyskała na to stosowną zgodę.
* Uprawnienia do systemów informatycznych służących do przetwarzania danych osobowych nadawane są wyłącznie osobom posiadającym stosowne upoważnienie do przetwarzania danych osobowych.
* Użytkownicy systemu informatycznego przetwarzającego dane osobowe wykorzystują w procesie uwierzytelnienia identyfikatory (loginy) i hasła.
* Użytkownik zobowiązany jest do:
* niezapisywania haseł, w szczególności ich nieumieszczania w miejscach dostępnych dla osób trzecich;
* nieujawniania hasła innym osobom;
* zachowania hasła w tajemnicy, również po jego wygaśnięciu;
* przestrzegania zasad dotyczących jakości i częstotliwości zmian hasła;
* wprowadzania hasła do systemu w sposób minimalizujący podejrzenie go przez osoby trzecie;
* szyfrowania plików przekazywanych drogą elektroniczną.
* Hasła powinny składać się z co najmniej 8 znaków (małe, wielkie litery, przynajmniej jedna cyfra lub znak specjalny).
* Każdy komputer powinien zostać wyposażony w legalny, licencjonowany program antywirusowy.
* Każdy komputer powinien mieć automatyczny wygaszacz ekranu, w przypadku czasowego przestoju pracy, tak aby chociaż przy krótkiej nieobecności pracownika osoba nieuprawniona nie miała możliwości dostępu do danych. Stosowanie się do wprowadzonych haseł do odblokowania wygaszaczy ekranu.
* W przypadku wykorzystania nośników typu pendrive i przechowywania na nich danych osobowych należy bezwzględnie zaszyfrować takie nośniki.