M7 – Ochrona

Mikołaj Wiszenko

# Wymagania funkcjonalne

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Nazwa** | **Opis** | **Prio.** |
| 1 | Uprawnienia | Każda osoba chcąca dostać się do budynku musi mieć odpowiednie uprawnienia. | 8 |
| 1.1 | Nadawanie uprawnień | Możliwość przydzielenie odpowiednich uprawnień do wybranej osoby. | 8 |
| 1.2 | Zmiana uprawnień | Możliwość zmiany przydzielonych uprawnień do wybranej osoby. | 5 |
| 1.3 | Zdalne otwieranie | Ochrona budynku może otworzyć dowolne drzwi przy pomocy konsoli. | 4 |
| 2 | Walidacja dostępu | Sprawdzanie czy dana osoba posiada uprawnienia do danego obszaru. | 8 |
| 2.1 | Sprawdzenie dostępu | Odczytanie uprawnień do danego pomieszczenia przy pomocy karty dostępu. | 8 |
| 2.2 | Udzielenie dostępu | Dla odpowiedniej karty dostępowej, otwarcie drzwi do danego pomieszczenia | 8 |
| 2.3 | Odmowa dostępu | Nie otwarcie drzwi na kartę dostępową bez odpowiednich uprawnień. | 8 |
| 3 | Raporty | Wgląd do danych. | 5 |
| 3.1 | Analiza incydentów | Lista incydentów nieuprawnionego dostępu. | 3 |
| 3.2 | Sprawdzenie dostępności obszaru | Sprawdzenie czy dany obszar w danym dniu i w przedziale czasowym jest zajęty | 8 |
| 4 | Monitoring | Zarządzanie kamerami obiektu. | 7 |
| 4.1 | Dostęp do podglądu | Możliwość oglądania w czasie rzeczywistym obrazu z kamer szkolnych. | 7 |
| 4.2 | Nagrywanie | Nagrywanie obrazu z kamer z możliowością przechowywania do określonego czasu. | 3 |
| 5 | Pomieszczenia | Spis pomieszczeń. | 9 |
| 5.1 | Lista pomieszczeń | Możliwość wyświetlenia listy pomieszczeń. | 9 |
| 5.2 | Zarządzanie pomieszczeniem | Możliwość dodania, edycji i usunięcia pomieszczenia. | 8 |
| 5.3 | Rezerwacja pomieszczenia | Możliwość zarezerwowania pomieszczenia na dany dzień i godzinę. | 7 |
| 5.4 | Blokowanie pomieszczenia | Możliwość zablokowania i odblokowania pomieszczenia w określonym celu. | 7 |

# Wymagania niefunkcjonalne

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Nazwa** | **Opis** | **Prio.** |
| 1 | Manualny dostęp | W razie awarii systemu, ochrona obiektu może ręcznie otwierać drzwi. | 8 |
| 2 | Szybka reakcja na uprawniony dostęp | Osoba która chce wejść do obszaru z uprawnieniami, pod odbiciu identyfikatora nie powinna czekać za długo. | 8 |
| 3 | Wymiana karty dostępowej | W razie zgubienia/zniszczenia/kradzieży jest możliwość wydania nowej. | 7 |
| 4 | Intuicyjny interfejs użytkownika | Użytkownik powinien intuicyjne rozpoznawać interfejs, aby nie było niepotrzebnych wątpliwości podczas jego użytkownika. | 8 |
| 5 | Bezpieczeństwo danych | W razie awarii systemu bądź jego części dane użytkowników nie zostaną przypadkowo zmienione. | 8 |
| 6 | Minimalizacja ryzyka niepowołanego dostępu | W razie awarii systemu ilość incydentów związanych z niepowołanym dostępem powinna być zminimalizowana. | 6 |

Zapotrzebowanie z innych modułów

* M2 – Ewidencja (Żaneta Pająk) - Lista osób: ID 12.2
* M10 – Kadry (Adrian Nartowicz) - Lista pracowników: ID 3.3
* M7 – Technicy (Artur Pazik) - Lista prowadzonych prac
* M4 – Plan Lekcji (Jacek Smoliński) - Lista zajęć: ID 8.4

# Udziałowcy modułu

* M4 – Plany Lekcji (Jacek Smoliński) - ID 3.2 dostępność pomieszczenia
* M13 – Egzaminy maturalne (Tomasz Skiba) - ID 3.2 dostępność pomieszczenia
* M5 – Program nauczania i zajęcia pozalekcyjne (Mikołaj Gregorczyk) - ID 3.2 dostępność pomieszczenia
* M7 – Technicy (Artur Pazik) - ID 3.2 dostępność pomieszczenia

# Przypadek użycia

**Nazwa:** Nadanie uprawnień

**Kontekst użycia:** Użytkownik posiada nowe uprawnienia.

**Zakres i poziom:** Moduł Ochrony (7) oraz urządzenia sterujące zamkiem drzwi.

**Aktor główny:** Użytkownik uprawniony do nadawania dostępów (administrator).

**Pozostali aktorzy i udziałowcy:** Użytkownik, któremu nadajemy dostęp oraz system.

**Wyzwalacze / inicjacja:** Otwarcie formatki do nadawania dostępu.

**Warunki początkowe:** Administrator jest zalogowany do systemu.

**Warunki końcowe:**

* **Gwarancje powodzenia:** Użytkownik otrzymał dodatkowe uprawnienia.
* **Minimalne gwarancje:** Dane użytkowników nie zostaną zmienione oraz system będzie sprawny.

**Główny scenariusz powodzenia / przepływ podstawowy:**

1. Administrator otwiera formatkę do *Nadawania uprawnień*.
2. Administrator wybiera odpowiedniego użytkownika.
3. Administrator wybiera odpowiednie uprawnienia.
4. Administrator zapisuje zmianę.
5. System przetwarza żądanie.
6. System informuje administratora o powodzeniu.

**Przepływy alternatywne:**

2. Użytkownika nie ma w bazie.

2.1. Administrator nie może ukończyć zadania.

3. Wymaganych uprawnień nie ma w systemie.

3.1 Administrator nie może ukończyć zadania.

6. System napotkał błąd.

6.1. System informuje administratora o błędzie.

**Punkty rozszerzenia:**

**Specjalne wymagania:**

**Dodatkowe informacje:**