1. Definicje struktury firmy:

- główny administrator - administrator stanowiący pieczę nad pozostałymi administratorami
- administrator - osoba zarządzająca przydzielonymi segmentami aplikacji
- pracownik - osoba wykonująca polecenia administratorów
- użytkownik - osoba korzystająca z systemu aplikacji

2. Definicja bezpieczeństwa.

Przez bezpieczeństwo informacji w systemach IT rozumie się zapewnienie:

- Poufności informacji (uniemożliwienie dostępu do danych osobom trzecim).
- Integralności informacji (uniknięcie nieautoryzowanych zmian w danych).
- Dostępności informacji (zapewnienie dostępu do danych, w każdym momencie żądanym przez użytkownika, pod warunkiem spełniania technicznych wymagań)

Administrator aplikacji stosuje adekwatne do sytuacji środki aby zapewnić bezpieczeństwo informacji w Firmie.

- Oznaczanie danych

Jako dane podlegające szczególnej ochronie (informacje poufne) rozumie się:

- informacje o realizowanych zakupach (zarówno zawartość koszyka klienta, historię zakupów),
- dane dostępowe do systemów IT,
- dane osobowe,
- inne informacje oznaczone jako „informacji poufne" lub „dane poufne".

- Zasada minimalnych uprawnień
  Każdy użytkownik ma dostęp do minimalnych uprawnień potrzebnych do dokonania zakupów lub skorzystania z bazy danych sklepu. Administratorzy posiadają szersze uprawnienia, odpowiednie do funkcji jaką pełnią w administracji sklepu.
  Innymi słowy: każdy administrator powinien posiadać tylko takie uprawnienia jakie są wymagane do realizacji swoich obowiązków.
- Zasada wielowarstwowych zabezpieczeń
  Aplikacja powinna być chroniona równolegle na wielu poziomach. Zapewnia to pełniejszą oraz skuteczniejszą ochronę danych.
  Przykładowo: w celu ochrony przed atakami typu INJECTION stosuje się równolegle zabezpieczenia po stronie klienta oraz serwera.

1. **Zasada ograniczania dostępu**

Domyślnymi uprawnieniami w systemie aplikacji powinno być zabronienie dostępu. Dopiero w przypadku zaistnienia odpowiedniej potrzeby, administrator aplikacji przyznaje stosowne uprawnienia.
Przykładowo: domyślnie dostęp do bazy przechowującej dane klientów jest zabroniony. Stosowny dostęp zostaje przyznany osobie, której zajmowane stanowisko wiąże się z koniecznością pracy w tego typu systemie.

Wykorzystanie haseł

- Hasła użytkowników i administratorów powinny być okresowo zmieniane. System powinien o tym przypominać.

- Hasła nie mogą być przechowywane w formie otwartej (nie zaszyfrowanej).
- Hasła nie powinny być łatwe do odgadnięcia, to znaczy:
  - powinny składać się z minimum 9 znaków, w tym jeden znak specjalny
  - nie mogą przybierać prostych form, np. 123456789, stanislaw, dom99, haslo, Magda8, itp.
- Hasła mogą być tworzone według łączenia „losowych" (tj nie istniejących w popularnych słownikach) sylab/słów, np,: mal-tra-laza-#topa. W ten sposób można uzyskać długie hasło stosunkowo proste do zapamiętania.

Odpowiedzialność pracowników za dane poufne

Każdy pracownik odpowiada za utrzymanie w tajemnicy danych poufnych, do których dostęp został mu powierzony.

- **Monitoring bezpieczeństwa**

W celu zapewnienia ochrony informacji administrator odpowiedzialny za ochronę bazy danych może stosować monitoring wykorzystania bazy danych, w szczególności obejmujący następujące elementy:

- analiza oprogramowania z jakiego łączy się użytkownik,
- analiza czasu dostępu do bazy,
- analiza wszelakich dostępów (autoryzowanych oraz nieautoryzowanych) do bazy danych,
- analiza prób złamania zabezpieczeń bazy danych,
- analiza aplikacji przez Google Play.

Monitoring bezpieczeństwa musi odbywać się z zachowaniem obowiązującego prawa.

1. **Edukacja pracowników w zakresie bezpieczeństwa**

Właściciele aplikacji dbają o cykliczną edukację pracowników w zakresie bezpieczeństwa informacji. Pracownicy w zależności od zajmowanego stanowiska mogą uczestniczyć w szkoleniach z zakresu:

- ochrony Danych Osobowych,
- świadomości istnienia problemów bezpieczeństwa,
- szczegółowych aspektów bezpieczeństwa.

Odpowiedzialność pracowników za dane dostępowe do systemów

Każdy administrator zobowiązany jest do ochrony swoich danych dostępowych do systemów informatycznych. Dane dostępowe obejmują między innymi takie elementy jak:

- hasła dostępowe,
- inne mechanizmy umożliwiające dostęp do systemów IT.

Przykłady ochrony danych dostępowych:

- nieprzekazywanie dostępów do systemów IT innym osobom (np. przekazywanie swojego hasła dostępowego osobom trzecim),
- nieprzechowywanie danych w miejscach publicznych (np. zapisywanie haseł dostępowych w łatwo dostępnych miejscach),
- Ochrona danych dostępowych przed kradzieżą przez osoby trzecie.

Transport danych poufnych przez pracowników

Zabrania się przenoszenia niezabezpieczonych danych poufnych. W szczególności zabrania się przenoszenia danych poufnych na nośnikach elektronicznych (np.: pendrive, nośniki CD).

1. **Korzystanie z infrastruktury IT aplikacji w celach prywatnych**

Zabrania się korzystania infrastruktury IT aplikacji w celach prywatnych.

1. **Systemy IT / serwery**
    - Systemy IT przechowujące dane poufne (np. dane osobowe) muszą być odpowiednio zabezpieczone.
    - W szczególności należy dbać o poufność, integralność danych przetwarzanych w systemach.
2. **Dokumentowanie bezpieczeństwa**

Administracja prowadzi dokumentacje w zakresie:

- obecnie wykorzystywanych metod zabezpieczeń systemów IT,
- ewentualnych naruszeń bezpieczeństwa systemów IT,
- dostępów do zbiorów danych / systemów udzielonych pracownikom.

1. **Dane osobowe**

Główny administrator ma obowiązek:

- ochrony danych (zabezpieczenia ich przed dostępem do nich osób trzecich),
- informacyjny wobec osób, których dane posiadamy (informowania, że mamy te dane i do jakich celów je wykorzystujemy),
- rejestracyjny (czyli zgłoszenia informacji o danych do rejestru prowadzonego przez GIODO).

1. **Testy systemu bezpieczeństwa aplikacji**
    - Wewnętrzna lub zewnętrzna weryfikacja bezpieczeństwa systemu (np. poprzez realizację testów penetracyjnych.
2. **Kopie zapasowe.**
    - Każde istotne dane (w tym dane poufne) powinny być archiwizowane na wypadek awarii w firmowej infrastrukturze IT.
    - Nośniki z kopiami zapasowymi powinny być przechowywane w miejscu uniemożliwiającym dostęp osobom nieupoważnionym.
    - Okresowo kopie zapasowe muszą być testowane pod względem rzeczywistej możliwości odtworzenia danych.
3. **Dostęp do systemów IT po rozwiązaniu umowy o pracę**

W przypadku rozwiązania umowy o pracę z pracownikiem, dezaktywowane są wszelakie jego dostępy w systemach IT.
Użytkownik po usunięciu konta traci dostęp do konta.

1. **Naruszenie bezpieczeństwa**

Wszelakie podejrzenia naruszenia bezpieczeństwa danych należy zgłaszać w formie ustnej lub za pośrednictwem poczty elektronicznej lub facebooka głównego administratora.
Każdy incydent jest odnotowywany w stosownej bazie danych, a główny administratora podejmuje stosowne kroki zaradcze.

1. **Weryfikacja przestrzegania polityki bezpieczeństwa.**

Główny administrator okresowo wykonuje wewnętrzny lub zewnętrzny audyt bezpieczeństwa mający na celu wykrycie ewentualnych uchybień w realizacji założeń polityki bezpieczeństwa.