## Security Requirements,

## Architectural ‌Risk Analysis,

## Security-oriented design

لیستی از requirementهای امنیتی و خطرات مربوط به آن‌ها، به علاوه لیستی از عملیات‌های زمان طراحی برای رفع آن خطرات و اطمینان از requirement مشخص شده:

* احراز هویت کاربران
  + استفاده از پسورد
  + ذخیره پسوردها به صورت hash شده با salt
  + اجبار کاربران به تغییر پسورد به صورت دوره‌ای، استفاده از history برای عدم تکرار پسورد‌ها
  + محدود کردن ورود پس از تعداد مشخصی تلاش ناموفق و اطلاع به کاربر
  + استفاده از جداول متفاوت برای ذخیره بازاریاب‌ها و اینفلوئنسر‌ها برای جداسازی اطلاعات
* اطمینان از هویت سرویس‌ها – مخصوصا شبکه‌های اجتماعی و APIهای مربوطه، بانک و پورتال‌های پرداخت – زمان رد و بدل اطلاعات
  + استفاده از SSL/TLS
  + محدود کردن و مشخص کردن ترافیک رد و بدل شده بین سیستم و آن‌ها
  + احراز هویت دو طرفه
* اطمینان از محرمانه بودن اطلاعات شخصی کاربران(هم اینفلوئنسرها، هم بازاریاب‌ها)
  + رمزنگاری
* حفاظت اطلاعات لاگین اینفلوئنسرها در شبکه‌های اجتماعی متفاوت
  + رمزنگاری
  + Access Control
* جلوگیری از حملات مربوط به دریافت ورودی از کاربر
  + Input Validation در تمامی فرم‌ها
* جلوگیری از حملات DoS
  + زمان‌بر بودن submit کردن فرم‌هایی که برای سرور کار زیادی دربردارند. مثلا، انجام جستجوها روی اینفلوئنسرها که از سمت سرور نیاز به اجرای الگوریتم‌‌های هوش مصنوعی سنگین‌ دارد، برای هر کاربر محدود شود (مثلا هر چند دقیقه یک درخواست.)
  + طراحی فرم‌ها به صورت چند مرحله‌ای و زمان‌بر برای کاربر (مثلا فرم ثبت درخواست، در چند مرحله انجام شود و تا پایان کامل هر مرحله، نیاز به درگیری کامل سرور نداشته باشد.)
  + استفاده از CAPTCHA در همه فرم‌ها.
* عدم دسترسی ادمین‌ها به اطلاعات حساس کاربران، محدود کردن دسترسی بعضی ادمین‌ها
  + استفاده از رمزنگاری
    - رمزنگاری جداگانه سیستم‌عامل و نرم‌افزارهای مشخص
    - ذخیره کلید‌ها به صورت سخت‌افزاری
  + Access Control
* امنیت log ها
  + عدم audit اطلاعات حساس
  + رمزنگاری فایل‌های log
* جلوگیری از انکار (repudiation)، مخصوصا در قراردادهای تبلیغات میان اینفلوئنسرها و بازاریاب‌ها
  + استفاده از امضای دیجیتال
  + استفاده از tokenهای مخصوص و تحویل آن‌ها به دو طرف (در قالب کد پیگیری)
* تازگی داده‌ها و تراکنش‌ها
  + استفاده از SSL/TLS