**User Requirement Specification (URS) for Data Breach Avoidance System**

**Document Revision:** 1.0  
**Date:** [Date]

**1. Introduction**

This URS provides detailed requirements for the development and implementation of a Data Breach Avoidance System tailored for the MyBankCardsManager application. The system will employ a combination of adaptive honeypot behaviors, intrusion detection systems, and user entity behavior analytics to enhance cybersecurity measures.

**2. System Overview**

The system focuses on proactive cybersecurity measures, including:

* Deploying sacrificial databases to distract attackers.
* Adaptive algorithms to improve honeypot behavior.
* Advanced threat detection mechanisms.
* Analyzing user behaviors to identify suspicious activities.

**3. User Requirements**

**3.1 Adaptive Honeypot Behavior Algorithm**

* The system must generate "genuine" honeypot data mimicking real data.
* The system must log intrusion attempts.
* The system should be able to analyze logged intrusion data and adapt honeypot behavior accordingly.
* The system should be able to regenerate honeypot data based on the analysis.

**3.2 Intrusion Detection System**

* The system should be able to detect unauthorized activities.
* It should employ signature-based or anomaly-based detection methods.

**3.3 User Entity Behavior Analytics**

* The system must maintain a database of known user behaviors.
* The system should analyze user behavior based on provided user code, password, and IP address.
* The system should be able to identify suspicious activities based on:
  + Unusual login times.
  + Unrecognized IP addresses.
  + Frequent login attempts.

**3.4 BankCardManager Application**

* The application should have a user interface to authenticate users.
* It should be able to send email alerts for potential intrusions.
* The application must interact with the database to retrieve and store data.
* The application should be able to drop, view, download, and add entries to the database.

**4. Functional Requirements**

**4.1 Adaptive Honeypot Behavior Algorithm**

* Functionality to generate initial honeypot data.
* Ability to log intrusion attempts with a timestamp.
* Functionality to analyze intrusion attempts and adapt honeypot behavior.

**4.2 Intrusion Detection System**

* Functionality to detect unauthorized activities.
* Ability to employ various detection methods.

**4.3 User Entity Behavior Analytics**

* Maintain a database of known user behaviors.
* Analyze user behaviors to identify suspicious activities.
* Maintain a history of user behaviors.

**4.4 BankCardManager Application**

* Authenticate users through a user interface.
* Send email alerts for potential intrusions.
* Interact with the database to perform CRUD operations.
* Implement routes for various application functionalities.

**5. Performance Requirements**

* The system should respond to user requests within 2 seconds.
* The system should be capable of handling up to 10,000 users concurrently.
* The system should send email alerts within 30 seconds of detecting an intrusion attempt.

**6. Security and Compliance**

* All user data must be encrypted.
* The system should comply with GDPR and other relevant data protection regulations.

**7. Scalability**

* The system should be scalable to accommodate increasing user numbers and data volume.

**8. Backup and Recovery**

* Regular backups of the database should be taken.
* There should be a provision for data recovery in case of system failures.