**Game Design Document - ACCESS DENIED**

**1. Overview**

**1.1 Game Concept**

ACCESS DENIED is an engaging cybersecurity awareness game developed on behalf of the Municipality of Amsterdam. The game aims to educate players about cybersecurity threats, best practices, and consequences through interactive challenges and simulated real-life scenarios.

**1.2 Target Audience**

The primary target audience for ACCESS DENIED includes employees and residents of Amsterdam who have varying levels of knowledge about cybersecurity. The game is designed to be accessible and enjoyable for players of all skill levels.

**1.3 Game Objectives**

* Raise awareness about cybersecurity threats and best practices.
* Educate players about the consequences of cybersecurity mistakes.
* Enhance players' critical thinking and decision-making skills in cybersecurity scenarios.

**2. Gameplay**

**2.1 Core Gameplay Mechanics**

* Players will engage in a series of tasks related to cybersecurity, including answering true or false questions and managing virtual emails.
* The game will present players with a set of true or false questions related to cybersecurity, challenging their knowledge and understanding of common threats and best practices.
* Players will manage a virtual inbox containing both malicious and non-malicious emails. They must assess the emails' maliciousness and perform appropriate actions like forwarding or deleting them.
* Incorrect answers to questions or mishandling of emails will result in consequences, such as screen freezing or pop-ups, to simulate real-life repercussions of cybersecurity mistakes.
* Players will earn points for correct answers and successful email management, with a timer adding an element of urgency to complete tasks within a specified time frame.

**2.2 Multiplayer Mode (Potential Future Enhancement)**

* "ACCESS DENIED" may include a multiplayer mode where one player acts as the hacker and other players act as defenders.
* The hacker player will attempt to infiltrate the defenders' systems by sending malicious emails or exploiting vulnerabilities.
* The defender players must correctly answer questions and manage emails to prevent successful cyberattacks.
* Successful defence or infiltration will earn points for the respective players.

**3. Visual Style and User Interface**

**3.1 Visual Style**

The game will have a visually appealing and intuitive user interface with a modern and professional aesthetic. The visual style should effectively convey the cybersecurity theme and create an engaging atmosphere for the players.

**3.2 User Interface**

* The user interface will feature clear and concise elements, including question prompts, answer choices, email management controls, and score displays.
* Feedback mechanisms such as notifications, pop-ups, and visual effects will be used to provide immediate feedback to the players' actions.

**4. Monetization (Optional)**

"ACCESS DENIED" may incorporate monetization strategies to support its development and ongoing maintenance. Potential monetization options include:

* In-app purchases for additional game content or customization options.
* Advertisements displayed during game sessions.
* Premium version offering enhanced features or additional levels.

**5. Technical Specifications**

**5.1 Target Platform**

* The game is primarily developed for desktop platforms, including Windows, macOS, and Linux.
* Compatibility with web browsers may also be considered for wider accessibility.

**5.2 Development Tools and Technologies**

* Unity Game Engine [Version 2022.2.6f1]
* C# Programming Language
* Git for version control
* Additional libraries and frameworks as necessary (e.g., Photon Unity Networking for multiplayer mode)

**6. Release Plan**

**6.1 Milestones**

* Milestone 1: Basic gameplay mechanics and user interface implementation.
* Milestone 2: Question system and email management functionality.
* Milestone 3: Implementation of consequences for incorrect answers and email mismanagement, scoring system, and timer functionality.
* Milestone 4: Visual enhancements, sound design, and polish.
* Milestone 5: Testing and debugging to ensure smooth gameplay experience.
* Milestone 6: Potential development of multiplayer mode using Photon Unity Networking (if applicable).
* Milestone 7: Final testing, bug fixing, and optimization.
* Milestone 8: Release preparations, including packaging, distribution, and marketing materials.

**6.2 Release Timeline**

The release timeline will be divided into the following phases:

* Pre-production: [20-03-2023] - [25-03-2023]
  + Concept development, initial design, and technical planning.
* Production: [26-03-2023] - [19-05-2023]
  + Milestones 1-7 will be completed during this phase, ensuring that all gameplay mechanics, features, and content are implemented.
* Post-production: [20-05-2023] - [26-05-2023]
  + Final testing, bug fixing, optimization, and preparations for the release.

**6.3 Quality Assurance**

* Testing will be conducted at each milestone to identify and address any bugs, glitches, or gameplay issues.
* The game will undergo comprehensive playtesting by both the development team and external testers to ensure a smooth and enjoyable player experience.

**6.4 Updates and Support**

* Regular updates will be provided to address any issues, introduce new content, and incorporate player feedback.
* Ongoing technical support will be offered to address user inquiries and maintain the game's functionality on supported platforms.

**Conclusion**

This Game Design Document outlines the key aspects of ACCESS DENIED, including its concept, gameplay mechanics, visual style, technical specifications, and release plan. By following this document, the development team can create an engaging and educational cybersecurity awareness game.