BlinkID

Version 3.0

Document Preparation

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Role** | **Approval (Signature)** | **Approval Date** |
| Himaadithi Lethakula | Project Requirements Manager | Himaadithi Lethakula | 04/22/24 |
| Vyshnavi Balabhadruni | Project Design Manager | Vyshnavi Balabhadruni | 04/22/24 |

Document Approvals

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Role** | **Approval (Signature)** | **Approval Date** |
| Akash Rao Sudati | Project Configuration Manager | Akash Rao Sudati | 04/22/24 |
| Mounika Reddy Dubba | Project Quality Assurance and Configuration Manager | Mounika Reddy Dubba | 04/22/24 |
| Venkata Sai Ramya Padmasri Boggaram | Project Technical Manager | Venkata Sai Ramya Padmasri Boggaram | 04/22/24 |
| Varun Vanaparthi | Project Manager | Varun Vanaparthi | 04/22/24 |

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
| 02/09/2024 | 1.0 | The first draft | Himaadithi Lethakula,  Vyshnavi Balabhadruni |
| 04/09/2024 | 2.0 | The draft with additional purposes, review features and constrains | Venkata Sai Ramya Padmasri Boggaram |
| 04/22/2024 | 3.0 | The draft with various formatting and reviewed table of contents and added changes to stakeholder and user description. | Venkata Sai Ramya Padmasri Boggaram |

Table of Contents

1. [Introduction](#_Introduction) 5

1.1 [Purpose of the Document](#_Purpose_of_the) 5

1.2 [Scope of the Document](#_Scope_of_the) 5

1.3 [References](#_References) 5

1.4 [Definitions, Acronyms, and Abbreviations](#_Definitions,_Acronyms,_and) 5

2. [Positioning](#_Positioning) 6

2.1 [Business Opportunity](#_Business_Opportunity) 6

2.2 [Problem Statement](#_Problem_Statement) 6

2.3 [Product Position Statement](#_Product_Position_Statement) 7

3. [Stakeholder and User Descriptions](#_Stakeholder_and_User) 7

3.1 [Stakeholder Summary](#_Stakeholder_Summary) 7

3.2 [User Summary](#_User_Summary) 7

3.3 [User Environment](#_User_Environment) 7

3.4 [Summary of Key Stakeholder or User Needs](#_Summary_of_Key) 8

3.5 [Alternatives and Competition](#_Alternatives_and_Competition) 9

4. [Product Overview](#_Product_Overview) 9

4.1 [Product Perspective](#_Product_Perspective) 9

4.2 [Assumptions and Dependencies](#_Assumptions_and_Dependencies) 9

4.3 [Cost and Pricing](#_Cost_and_Pricing) 10

4.4 [Licensing and Installation](#_Licensing_and_Installation) 10

5. [Product Features](#_Product_Features) 10

5.1 [Feature 1 – Facial Recognition Authentication](#_Facial_Recognition_Authentication:) 10

5.2 [Feature 2 – Access Control Integration](#_Access_Control_Integration:) 10

5.3 [Feature 3 – User Interface Design](#_User_Interface_Design:) 11

5.4 [Feature 4 – Mobile Compatibility](#_Mobile_Compatibility:_Ensure) 11

5.5 [Feature 5 – Integration with Existing Systems](#_Integration_with_Existing) 11

5.6 [Feature 6 – Customizable Security Policies](#_Customizable_Security_Policies:) 11

5.7 [Feature 7 – Continuous Updates and Support](#_Continuous_Updates_and) 11

5.8 [Feature 8 – User Training and Education](#_User_Training_and) 11

5.9 [Feature 9 – Remote Management](#_Remote_Management:_Enable) 11

5.10 [Feature 10 – Integration with Student Services](#_5.10_Integration_with) 11

6. [Constraints](#_Constraints) 11

7. [Quality Ranges](#_Quality_Ranges) 12

8. [Precedence and Priority](#_Precedence_and_Priority) 12

9. [Other Product requirements](#_9._Other_Product) 13

Project Vision Documentation

# Introduction

## Purpose of the Document

This Vision Document is designed to offer a comprehensive overview of the BlinkID project, focusing on the integration of facial recognition technology within the Smart Campus initiative. The primary objective is to gather, analyze, and define the high-level requirements and features essential for the successful implementation of BlinkID. By delineating the needs of stakeholders and target users, this document elucidates the rationale behind these requirements and how BlinkID aims to fulfill them.

## Scope of the Document

This document serves as an overview of the BlinkID project, covering its inception, intended functionality, operational context, and potential deployment strategies. In order to ensure alignment and productive engagement throughout the project's lifecycle, it seeks to give stakeholders an overview of the project's scope, objectives, and boundaries.

## References

# 1.Zhang, Y., Zhang, W., & Xiong, N. N. (2018). Smart Campus with Facial Recognition and Tracking. In Proceedings of the International Conference on Smart Computing and Communication (pp. 292-302). Springer, Cham.

# 2.Sharma, A., & Kaur, M. (2021). Facial Recognition Technology for Smart Campus Security. In Proceedings of the International Conference on Artificial Intelligence, IoT, and Digital Technology (pp. 165-177). Springer, Singapore.

# Zhang, H., Shao, M., & Li, M. (2019). Design and Implementation of Smart Campus Based on Facial Recognition Technology. In Proceedings of the International Conference on Intelligent Transportation, Big Data & Smart City (pp. 233-240). Springer, Singapore.

# Project\_smart\_campus\_PPD\_version\_2( <https://drive.google.com/file/d/1k0n1DCK70Ez_OurQhA22LG9MwKlwD7so/view?usp=drive_link>)

# Project\_smart\_campus\_Project\_vision\_Document\_version\_2(<https://drive.google.com/file/d/1sNEibsJLEY_eJ1BWT9CaKe5C81u5NqAZ/view?usp=drive_link>)

# Project\_smart\_campus\_SDD\_version\_2(<https://drive.google.com/file/d/1VtA0Jfs0HiZzkVKC_BNsphXsSO37Zltw/view?usp=drive_link>)

# Project\_smart\_campus\_Software\_Test\_Document\_(STD)\_version\_2(<https://drive.google.com/file/d/1PrSeEJN5LjtrF04M8tCuSCU4CEn7TSg4/view?usp=drive_link>)

# Project\_smart\_campus\_SRS\_version\_2(<https://drive.google.com/file/d/1rkHd3ZsuzLRmns8lIaKHoTFJ3oYld3_4/view?usp=drive_link>)

## Definitions, Acronyms, and Abbreviations

|  |  |  |
| --- | --- | --- |
| **Term** | **Abbreviation / Acronym** | **Definition** |
| BlinkID | - | The proposed facial recognition system for Smart Campus security. |
| Facial Recognition Technology | FRT | Technology capable of verifying or identifying a person from a digital image or video frame. |
| Biometric Authentication | - | A security process that relies on the unique biological characteristics of an individual. |
| Access Control | - | A system that manages access to resources by granting or denying requests based on user credentials. |
| Examination Proctoring | - | The use of technology to monitor students during examinations. |

# Positioning

## Business Opportunity

The BlinkID initiative presents a unique opportunity to leverage cutting-edge facial recognition technology for the transformation of campus administration and security. By integrating advanced biometric capabilities, BlinkID offers the potential for enhanced safety procedures and operational efficiencies within academic settings. This initiative addresses the critical need for robust security measures and streamlined identification verification processes in educational institutions.

## Problem Statement

|  |  |
| --- | --- |
| The problem of | Addressing illegal access and identity fraud in academic institutions is indeed crucial for maintaining security and integrity. |
| affects | The students/ staff/ administrators /individuals who are in academic institutions, cause and want to raise effective methods to enhance security and integrity of academic institutions. |
| the impact of which is | Illegal access and identity fraud in academic institutions can lead to various adverse consequences, including compromised safety, potential financial losses, and diminished trust in the security measures implemented by the university. |
| a successful solution would be | A successful solution would be one that seamlessly integrates with the existing infrastructure, ensures privacy, provides reliable and rapid identification, and fosters a secure environment for all stakeholders. |

## Product Position Statement

|  |  |
| --- | --- |
| For | For educational institutions that require high level security and efficient identity management |
| Who | Redefines campus security through advanced facial recognition, ensuring smooth access control and heightened safety measures. With a user-centered approach, BlinkID sets a new standard for modern security solutions, prioritizing efficiency and peace of mind for all stakeholders. |
| The BlinkID | Is a Android Based Application |
| That | Crafted to revolutionize campus security and access control, empowering users with cutting-edge facial recognition technology for seamless and secure identification, ultimately fostering a safer and more efficient environment for all. |
| Unlike | Other biometric web-based or applications |
| Our product | By employing advanced facial recognition technology, it simplifies authentication processes, ensuring swift and secure access for authorized individuals. With a focus on user-centric design, BlinkID fosters a positive user experience, minimizing the need for extensive user research and engagement. It serves as a comprehensive platform, offering a one-stop solution for campus security needs, including identity verification, access control, and real-time monitoring. By verifying user identities and ensuring compliance with security protocols, BlinkID addresses concerns related to trust and transparency, providing peace of mind to administrators and users alike. |

# Stakeholder and User Descriptions

## Stakeholder Summary

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Description** | **Responsibilities** | **Stakeholder** |
| University Administration | Oversees the entire BlinkID project implementation. | Ensures the project aligns with institutional goals.  Approves funding.  Monitors project progress. | Decision-maker |
| IT Department | Manages the technical infrastructure of BlinkID. | Ensures system integration with current IT setup. Manages data privacy and security concerns | Technical implementer |
| Security Personnel | On-ground enforcers of the BlinkID system. | Operates and monitors the system.  Responds to security alerts. | End-user |
| Students and Faculty | Primary users of the BlinkID system for campus access. | Utilize the system for daily access.  Provide feedback for system improvements | Beneficiary |

## User Summary

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Description** | **Responsibilities** | **Stakeholder** |
| Student | Regular user of campus facilities. | Uses BlinkID for access.  Follows security protocols. | Beneficiary |
| Faculty Member | Accesses academic buildings and offices. | Uses system for room access.  Integrates system in teaching methods. | Beneficiary |
| Administation and Security wing | Ensures campus safety. | Monitors entrances.  Manages incident response. | Operator |

## User Environment

|  |  |
| --- | --- |
| **Aspect** | **Description** |
| Number of People | The system is designed to accommodate a university environment with a diverse range of users, including current students, faculty, staff members, alumni, and visitors. |
| Task Cycle Length | Task cycles within the university environment can vary significantly in length, from several minutes for activities like enrollment or course registration to seconds for authentication tasks. |
| Time Spent in Activities | Activities such as enrollment or course registration typically take a few minutes, while authentication for accessing campus facilities or online resources is usually completed within seconds. System navigation time can vary depending on the complexity of the task and user familiarity. |
| Environmental Constraints | The system is primarily used in indoor environments on the university campus but may also be used in outdoor or mobile settings for access control tasks or events. |
| System Platforms | The system supports a wide range of platforms, including desktop computers, laptops, tablets, and smartphones, with compatibility for both web-based and mobile applications. |
| Integration Requirements | Integration with existing campus systems, including student information systems, access control systems, library systems, and other campus resources, is essential for effective functionality. The system must also comply with relevant data protection regulations and privacy guidelines. |

## Summary of Key Stakeholder or User Needs

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Stakeholder** | **Problem Description** | **Reasons for Problem** | **Current Solution** | **Solutions** | **Ranking** |
| Security Personnel | Lack of Security: Inadequate authentication methods leading to security breaches. | Reliance on traditional ID cards, PIN codes, or passwords. | Traditional ID cards, PIN codes, or passwords. | Implement advanced biometric authentication (facial recognition) for enhanced security. | High |
| Administrative Staff | Inefficient Access Control: Manual verification processes causing delays and inefficiencies. | Security guards or receptionists manually verify IDs. | Security guards or receptionists manually verify IDs. | Implement automated access control systems with facial recognition technology. | High |
| IT and Development Team | Limited Personalization: Generic experiences fail to meet individual needs and preferences. | One-size-fits-all approach to services and recommendations. | One-size-fits-all approach to services and recommendations. | Develop a personalized recommendation engine based on facial recognition data. | Medium |
| Legal and Compliance Team | Compliance Concerns: Current methods may not align with data protection regulations. | Ad hoc data handling processes without robust compliance measures. | Ad hoc data handling processes without robust compliance measures. | Ensure BlinkID complies with relevant data protection regulations and privacy guidelines. | High |

## Alternatives and Competition

|  |  |  |  |
| --- | --- | --- | --- |
| **Product or Solution** | **Description** | **Strengths** | **Weaknesses** |
| Manual ID Verification | Traditional methods relying on physical ID cards. | - Familiarity and simplicity for users - No technological dependencies | - Prone to human error - Inefficient for large-scale operations - Limited security features |
| Access Control Systems | Systems from companies like HID Global, LenelS2, and Tyco, using keycards, PIN codes, or biometric authentication. | - Established infrastructure in some environments - Relatively low-cost implementation | - Vulnerable to theft or misuse of access credentials - Lack of biometric authentication - Limited flexibility and scalability |
| Facial Recognition Solutions | Solutions from companies such as FaceFirst, NEC, and Cognitec, providing advanced biometric authentication using facial recognition technology. | - Advanced biometric authentication for enhanced security - Seamless user experience with quick verification | - Potential concerns over privacy and data protection - Implementation costs may be higher - Technical challenges in accuracy and reliability |
| Mobile Authentication Apps | Apps like Google Authenticator, Microsoft Authenticator, and Authy, providing two-factor authentication (2FA) using mobile devices for enhanced security. | - Convenience and portability - Integration with existing mobile technology | - Security vulnerabilities in mobile devices - Dependency on battery life and network connectivity - Limited adoption in some user demographics |
| Biometric Authentication Systems | Systems from companies like BIO-key, Idemia, and Aware, using fingerprint, iris, or voice recognition for authentication. | - High level of security with biometric authentication - Difficult to replicate or forge | - Privacy concerns related to biometric data storage and usage - Cost of implementation and maintenance - Technical challenges in accuracy and reliability |

# Product Overview

## Product Perspective

BlinkID assumes a strategic role as a pivotal component within the overarching campus security ecosystem. Meticulously engineered, it seamlessly aligns with existing school security protocols, student information systems, and facility management technologies. Operating as a supplementary feature rather than a substitute, BlinkID harmonizes with pre-existing hardware and databases, necessitating minimal additional infrastructure. A comprehensive visual representation, encapsulated in a block diagram, elucidates the core components, their interconnections, and external interfaces for enhanced comprehension.

## Assumptions and Dependencies

BlinkID is designed to support Android devices. Currently, people using iOS phones are unable to access the application. However, once we convert the code to Swift programming, BlinkID will be available to iOS devices as well. Some other user interaction gestures and controls will be updated later to enhance the user experience.

The efficacy of BlinkID rests upon several foundational assumptions:

- Assurance of a robust network infrastructure and the availability of high-quality cameras.

- Seamless interoperability and harmonious interaction with the prevailing IT infrastructure.

- Rigorous adherence to data protection laws, ensuring legal compliance and safeguarding privacy.

- A continuous and reliable power supply, coupled with steadfast internet connectivity, to sustain uninterrupted operation.

Critical dependencies integral to the triumph of BlinkID include:

- Active cooperation from the campus community during the initial enrollment phase.

- Methodical and scheduled system updates and maintenance to guarantee sustained optimal performance.

## Cost and Pricing

Comprehensive cost considerations for BlinkID encompass various elements, software development, ongoing maintenance, and potential licensing fees.

**Cost Breakdown:**

|  |  |
| --- | --- |
| **Cost Element** | **Description** |
| Design | Creating wireframes, mockups, and UI designs tailored for educational institutions. Cost varies based on detail and complexity. |
| Development | Coding, testing, and integrating application components. Cost depends on hours required, team experience, and location. |
| Third-party Software and Tools | Purchasing or licensing third-party software and tools (e.g., student information systems, learning management systems) depending on required features. |
| Testing and Quality Assurance | Testing for bugs, errors, and usability to meet educational institution needs. |
| Launch and Ongoing Support | Launching the application, providing ongoing support, maintenance, and updates. |

**Pricing Strategy:**

|  |  |
| --- | --- |
| **Pricing Strategy** | **Description** |
| Subscription-based | Offering a flat fee per student or institution for access to BlinkID features. |
| Custom Pricing | Tailoring pricing based on student count, specific features, and support requirements. |
| Bulk Licensing | Providing discounted pricing for bulk purchases to encourage adoption across campuses or districts. |

## Licensing and Installation

BlinkID's licensing agreements will rigorously adhere to established software industry standards, ensuring the university holds requisite rights for widespread utilization. The installation process will be tactically orchestrated to minimize disruptions to campus operations, potentially scheduled during periods of low usage or academic breaks. Given the critical role licensing and installation play in optimizing the overall development effort, meticulous attention to these aspects is imperative throughout the design and implementation stages.

# Product Features

## Facial Recognition Authentication: Utilize advanced facial recognition algorithms for secure and seamless user authentication across campus facilities.

## Access Control Integration: Integrate BlinkID with existing access control systems to regulate entry to buildings, labs, and restricted areas.

## User Interface Design: Design intuitive user interfaces for administrators and end-users, facilitating easy enrolment, configuration, and usage of BlinkID features.

## Mobile Compatibility: Ensure mobile-friendly design and compatibility with various devices to provide convenient access to BlinkID functionalities on-the-go.

## Integration with Existing Systems: Enable seamless integration with other campus systems such as student databases and security infrastructure for enhanced functionality and data synchronization.

## Customizable Security Policies: Allow administrators to define and enforce customizable security policies, such as access permissions based on user roles or time-based restrictions.

## Continuous Updates and Support: Offer regular software updates and technical support services to ensure BlinkID remains up-to-date and functional at all times.

## User Training and Education: Provide comprehensive training resources and educational materials to ensure users understand how to effectively utilize BlinkID features while promoting best practices for security and privacy.

## Remote Management: Enable administrators to remotely manage BlinkID settings, user accounts, and access permissions for increased flexibility and convenience.

## 5.10 Integration with Student Services: Integrate with student services systems to provide additional functionalities such as course enrollment, academic advising.

# Constraints

**6.1 Integration of Systems:**

6.1.1 Limited Compatibility with Current Systems: BlinkID's utility and efficacy may be constrained by difficulties connecting with different campus systems.

6.1.2 Technical Complexity of Integration: It takes a lot of testing and development resources to integrate with different systems and protocols, which can cause delays and expenses.

6.1.3 Need for Seamless interaction: To maximize BlinkID's value and acceptance across campus facilities, it is imperative to ensure seamless interaction with the current infrastructure.

**6.2** **Technical Restrictions:**

6.2.1 Platform Compatibility: It takes a lot of testing and development work to ensure compatibility with different operating systems.

6.2.2 Performance Optimization: In order to keep BlinkID functioning well on a variety of devices and in a variety of network environments, optimization efforts are required.

**6.3** **Adherence to Regulations:**

6.3.1 Data Privacy Regulations: User consent procedures and safe data handling techniques are required to comply with data protection legislation.

6.3.2 Security Standards: In order to preserve compliance and safeguard user information, adherence to security standards is essential.

**6.4** **User Confidence:**

6.4.1 Transparent Data Handling: Gaining the trust of users requires open and honest information regarding data handling procedures.

6.4.2 Reputation Management: Upholding a favorable reputation via dependable service provision and prompt customer assistance.

**6.5 Trust and Credibility:**

6.5.1 Secure Biometric Data Handling: Ensuring user trust by employing robust encryption methods for the protection of biometric data and conducting all authentication processes securely.

6.5.2 Transparent Reporting: Building trust with users and institutions through transparent reporting on the use and storage of biometric data, enhancing credibility.

6.5.3 Continuous Improvement: Engaging with educational institutions for feedback and actively improving services, demonstrating a commitment to accountability and enhancement.

6.5.4 Reputation Building: Focusing on building trust and establishing a strong reputation in the field of biometric authentication and recognition, crucial for user and institutional adoption.

# Quality Ranges

Efficiency Enhancement:

* Ensure fast load times and smooth user interaction for optimal performance.
* Optimize resource usage and enable real-time processing for efficient operation.

Universal Adaptability:

* Support a wide range of devices and platforms, including Android and iOS.
* Utilize responsive design for consistent user experience across different screens.

Fortified Protection:

* Implement strong encryption and secure payment gateways to protect user data.
* Offer multi-factor authentication for enhanced security measures.

Sustainable Upkeep:

* Maintain effective version control and documentation for easy updates and management.
* Provide automated update mechanisms for timely delivery of bug fixes and new features.

# Precedence and Priority

|  |  |  |
| --- | --- | --- |
| **No.** | **Feature** | **Description** |
| 1 | User Enrollment | Ensure a seamless and user-friendly enrollment process to onboard users effectively onto the BlinkID platform. |
| 2 | Facial Recognition Authentication | Implement advanced facial recognition algorithms to provide secure and seamless user authentication across campus facilities. |
| 3 | Access Control Integration | Integrate BlinkID with existing access control systems to regulate entry to buildings, labs, and restricted areas. |
| 4 | User Interface Design | Design intuitive user interfaces for administrators and end-users, facilitating easy enrollment, configuration, and usage of BlinkID features. |
| 5 | Mobile Compatibility | Ensure mobile-friendly design and compatibility with various devices to provide convenient access to BlinkID functionalities on-the-go. |
| 6 | Integration with Existing Systems | Enable seamless integration with other campus systems such as student databases and security infrastructure for enhanced functionality and data synchronization. |
| 7 | Customizable Permissions | Allow administrators to define user roles and permissions based on their responsibilities and access needs within the BlinkID system. |
| 8 | Scalability | Design BlinkID with scalability in mind to accommodate growing user bases and evolving campus needs without compromising performance or security. |
| 9 | Continuous Updates and Support | Offer regular software updates and technical support services to ensure BlinkID remains up-to-date and functional at all times. |
| 10 | User Training and Education | Provide comprehensive training resources and educational materials to ensure users understand how to effectively utilize BlinkID features while promoting best practices. |

## 9. Other Product Requirements

**9.1 Applicable Standards**

* Legal and regulatory standards: Charitable Solicitation Laws, Electronic Communications Privacy Act (ECPA), California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR), Sarbanes-Oxley Act (SOX)
* Communications standards: OAuth (Open Authorization), Hypertext Transfer Protocol Secure (HTTPS), Secure Sockets Layer/Transport Layer Security (SSL/TLS), REST (Representational State Transfer)
* Platform compliance standards: Google Play Store Policies
* Quality and safety standards: ISO 27001 for information security management systems, Open Web Application Security Project (OWASP)

**9.2 System Requirements**

* The app must support the latest version of Android to ensure compatibility with the majority of mobile devices.
* A stable internet connection is required to process donations and provide real-time updates.
* Users must have Android mobile devices to use the application.

**9.3 Performance Requirements**

* The application is expected to be optimized for performance and free of significant bugs or issues that could negatively impact the user experience.
* This includes minimizing load times and ensuring that the app is responsive to user inputs.

**9.4 Environmental Requirements**

* Network connectivity: The strength and reliability of the network connection can affect the speed and accuracy of processing donations and displaying information.
* Hardware and software limitations: The hardware and software limitations of the user's device can impact the performance and compatibility of the app.
* Security: The security of the device and the network can impact the safety and security of user data and financial transactions.
* Resource availability: technical expertise, financial resources, time and project management, infrastructure and technology, and user feedback and engagement are key resources that can impact the development process and the final product.

**9.5 Documentation Requirements**

* + Other documents required include, but are not limited to:
  + Project Plan
  + Software Requirement Specification (SRS)
  + Software Design Document (SDD)
  + Software Test Document (STD)