Deliverable #1: Software Requirement Specification (SRS)

SE 3A04: Software Design II – Large System Design

Tutorial Number: T01

Group Number: G8

Group Members:

- Kyle Hagerman
- Michael Breau
- Zongcheng Li
- Jay Sharma
- Ahmed Al-Hayali

IMPORTANT NOTES

- Be sure to include all sections of the template in your document regardless whether you have something to write for each or not
  –If you do not have anything to write in a section, indicate this by the *N/A*, *void*, *none*, etc.

- Uniquely number each of your requirements for easy identification and cross-referencing

- Highlight terms that are defined in Section 1.3 (**Definitions, Acronyms, and Abbreviations**) with **bold**, *italic* or underline
- For Deliverable 1, please highlight, in some fashion, all (you may have more than one) creative and innovative features. Your creative and innovative features will generally be described in Section 2.2 (**Product Functions**), but it will depend on the type of creative or innovative features you are including.

1 Introduction

This SRS will provide an overview on software requirements for Secure Chat (**SC**), an Android Application. We documented the purpose of Secure Chat and our design decisions in this SRS, including the scope of the application, user characteristics, product requirements, use case diagrams and functional/non-functional requirements.

1.1 Purpose

This document details software requirements, a product description, and intended users and their use cases of **SC**. The document is intended for **SC** stakeholders, including but not limited to, project manager, domain experts, **SC** team members, investors, future users who work for the company, and company administrators.

1.2 Scope

The Secure Chat (**SC**) application is designed to facilitate secure communication within organizations that handle a large quantity of company trade secrets. The application provides a platform for employees to exchange sensitive information while ensuring confidentiality, integrity, and availability of data.

SC leverages a critical component that is responsible for establishing secure communication sessions. It also employs a protocol to verify the authorization of client users before granting access to the chat interface.

To enhance user experience, **SC** also offers message summarization. This feature allows users to receive summarized versions of lengthy messages, enabling them to stay updated with the company's current status even while on the go.

The primary goal of the application is to provide a highly secure communication platform that protects sensitive information from unauthorized access or interception. While prioritizing security, the application aims to provide a seamless and intuitive user experience, ensuring that employees can easily initiate and engage in secure conversations.

Ultimately, **SC** aims to deploy a scalable infrastructure that can effectively support the communication needs of a growing workforce.

1.3 Definitions, Acronyms, and Abbreviations

- **Design system**: A set of components, rules, style guides, and documentation used to build a coherent and on-brand interface of a product.
- **KDC**: A network component that helps control access within a network
- **LLM**: large language model
- **OS**: Operating system, used in reference to the operating system for different devices
- **SC**: Secure Chat, the name of the application that is being specified in this SRS
- **Responsive:** The ability for a user interface to adapt to various screen sizes

1.4 References

[PR-RA1] CSUCI, “Monthly Technology Maintenance Plan and Schedule”. https://www.csuci.edu/its/maintenance-schedule.htm. [Accessed: 6-March-2024].

[PR-SL1] Ramesh, Rohith. “The Significance of Testing Application Response Time.” *HeadSpin*, 9-June-2023, https://www.headspin.io/blog/how-to-test-application-response-time-for-overall-app-success. [Accessed: 1-March-2024].

[MS-M1] Gadhavi, Maitray. “What is Software Maintenance and Why is it Important for an Organization?”. *Radix*, 17-Dec-2023. https://cleancommit.io/blog/importance-of-software-maintenance-in-software-engineering/ [Accessed: 6-March-2024].

[SR-INT1] Aid, “Top 7 methods of data encryption in Android Applications,” Apriorit, 05-Sep-2022. [Online]. https://www.apriorit.com/dev-blog/612-mobile-cybersecurity-encryption-in-android. [Accessed: 9-Feb-2024].

[LR-COMP1] “PIPEDA Fair Information Principle 1 – Accountability - Office of the Privacy Commissioner of Canada.” https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_accountability/. [Accessed: 9-Feb-2024].

[LR-STD1] “Core app quality — Android Developers.” https://developer.android.com/docs/quality-guidelines/core-app-quality. [Accessed: 9-Feb-2023].

[LR-STD3] “User authentication guidance for information technology systems (ITSP.30.031 v3)”. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3#a21. [Accessed: 9-Feb-2023].

1.5 Overview

Section 2 contains the overall product description and provides the background knowledge required to understand the requirements. Section 3 contains the use case diagram for understanding the standard use cases for the system. Section 4 contains the business events that list the functional requirements and how their corresponding viewpoints interact with them in the system. Section 5 contains the non-functional requirements and the rationale for their inclusion. Section 6 discusses our main chosen innovative feature for the product as well as extra innovative features. The final section, section 7 includes the division of labor for deliverable 1.

2 Overall Product Description

2.1 Product Perspective

SC is a standalone internal communication software aimed to compartmentalize the company's sensitive information and isolate it from external actors. **SC**, similar to other commercial messaging applications, e.g., Slack, Telegram, or even WhatsApp, transmit messages, but also extends functionality to include the organization of business-centric meetings, and natural-language summaries of historical chat logs.

SC is to be installed on all company-issued Android devices to facilitate employee communication through secure channels. Administrator-provisioned credentials can be used to establish secure communication sessions protected by industry-standard authentication protocols.

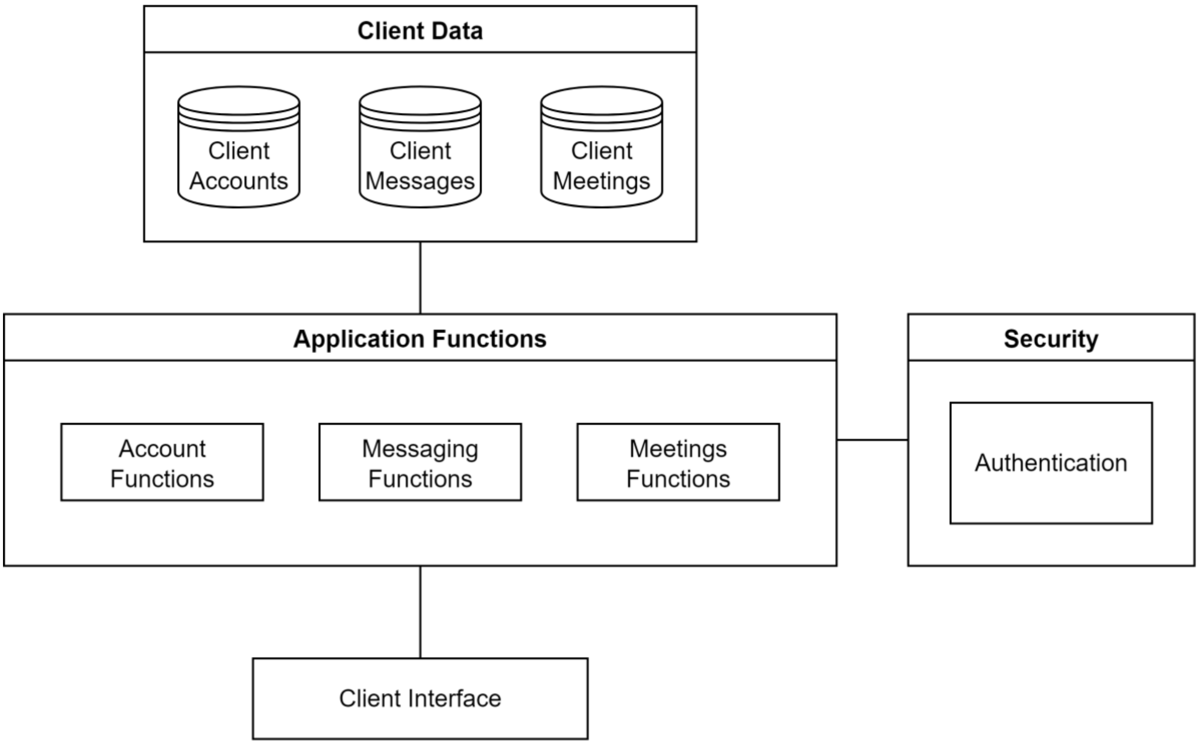

Figure 1. SC Block Diagram

2.2 Product Functions

The system allows users to message each other via secure connections, ensuring critical information is kept secret. There will be *four* modules in the product: the secure chat service, meeting service, account service, and personalization service. The major function is a secure chat service, which includes: sending messages, displaying chat history, requesting a chat history summary, and deleting chat history.

Within the meeting service, there are functions of scheduling a meeting, changing a meeting, canceling a meeting, and joining a meeting. Within the account service, there are functions of creating an account, logging in and logging out. Within the personalization service, there are functions to enable accessible color schemes, enable color blind mode, enable screen reading mode and magnify text.

Modules	**Functions**
Secure chat service	1. Send messages a. Allow the users to start a new secured chat. b. Allow the users to send messages to their colleagues with security. 2. Display chat history a. Allow users to see chat history. 3. Request a chat history summary a. Allows the user to generate a summary of their recent chat history with a given person. 4. Delete chat history a. Allow users to choose to delete chat history that they don't want.
Meeting service	1. Schedule a new meeting a. Allow users to schedule a new meeting. 2. Change an existing meeting a. Allow users to change an existing meeting. 3. Join a meeting a. Allow users to get notifications of all meetings they need to participate in. 4. Cancel a meeting a. Allow users to cancel a meeting scheduled by themselves.
Account service	1. Create account a. Allow employees to create an account. 2. Login a. Allow users to login with authentication. 3. Logout a. Allow users to log out safely.
Personalization service	1. Enable accessible color scheme a. Allow users to use high contrast colors. 2. Enable color blind mode a. Allow users to turn on color blind mode. 3. Enable screen reading mode a. Allow the user to turn on screen reading mode. 4. Magnify text a. Allow users to change their text magnification.

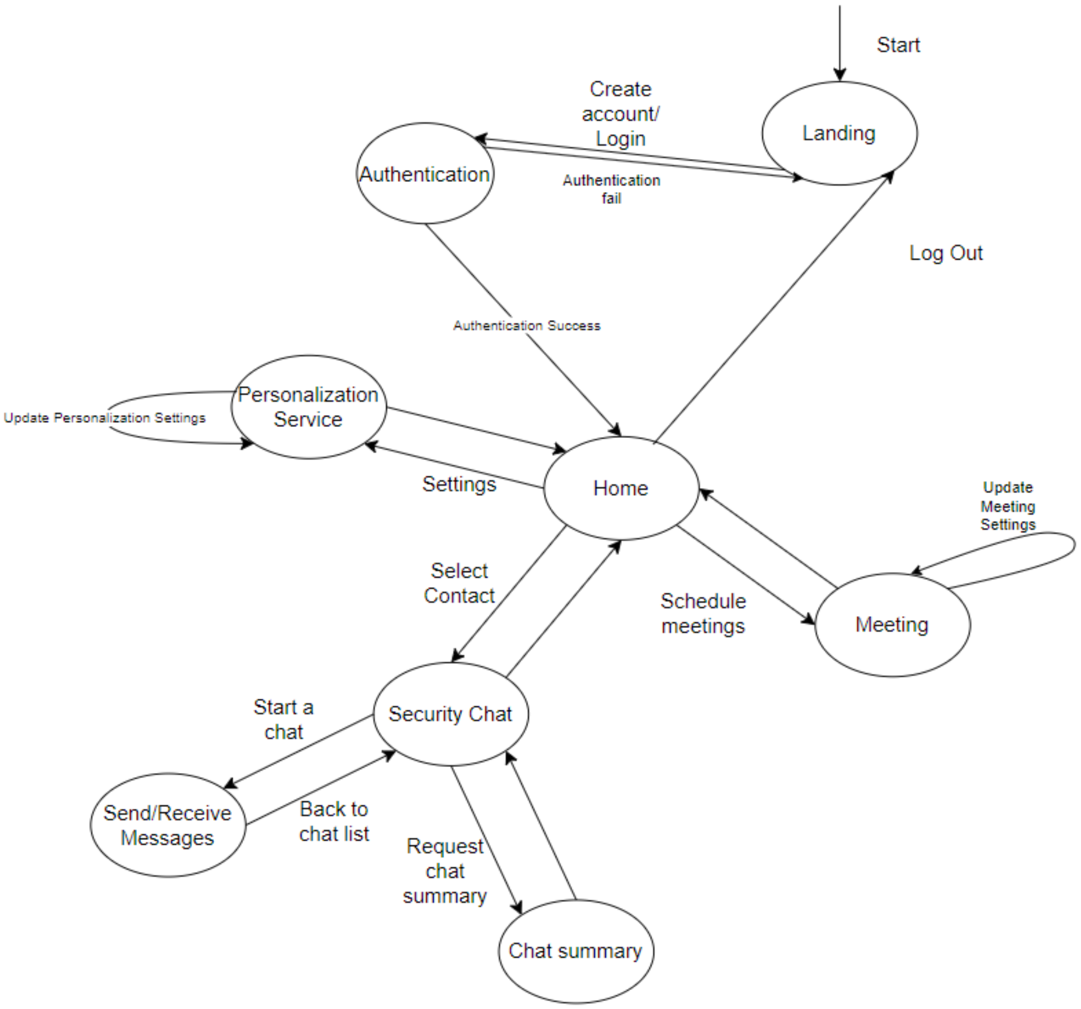

Figure 2. State Diagram

2.3 User Characteristics

Employee:

Educational Level:

- Employees are assumed to have basic skills of reading and writing. For those requiring accommodations with speech assistance, listening skills are assumed as well.

Experience:

- Any: the app is meant for all employees, therefore there will not be a restriction set in place.

Technical Expertise:

- Any: the app is meant for all employees, therefore there will not be a restriction set in place.

System Admin:

Educational Level:

- Completed an undergraduate degree.
- Assumed to have basic skills of reading and writing.

Experience:

- Possess ≥ 2 years of relevant technical experience.

Technical Expertise:

- Be familiar with the tech stack.

Maintenance:

Educational Level:

- Assumed to have basic skills of reading and writing.

Experience:

- Considerable technical experience with the tech stack used (≥ 2 years).

Technical Expertise:

- Considerable expertise with the tech stack used.

2.4 Constraints

1. **System:** The system will include an app component to be located on employee phones and it must be on the android system.
2. **Security:** The system must be secure to ensure no leakage of company trade secrets, meaning no external libraries or systems which could take internal system data can be used.
3. **Security:** Chatting must take place over secure connection channels.
4. **Timeline:** The project must be completed by the week of April 8, 2024. As the project began in January, 2024, the time spent planning, testing, iterating, and gathering resources will be limited.
5. **Team size:** The team contains 5 aspiring software architects/developers from various technical backgrounds, thus the amount of time spent on the project is limited to the amount of work that 5 people can do. Planning must be done carefully to ensure unachievable levels of work (eg. planning for more features than feasible) are not expected for the final product.

2.5 Assumptions and Dependencies

- By having the chat logs securely stored on the server, the system should encrypt user messages from end to end.
- The client’s phones/devices will be able to run android applications.
- The chosen authentication and security systems have no known vulnerabilities that would compromise the security of the system.

- The application will only be used locally in Canada and therefore only needs to follow Canadian specific laws and regulations.

2.6 Apportioning of Requirements

- UH-PI1 - multiple language support and availability in different countries. For now, the system will be developed in English and be available at the headquarters of the client.
- PR-C1 - Accommodating 15000 users concurrently. Due to the scope of the project, the preliminary version will support 2 users using the chat interface.
- UH-EOU1, UH-L1, and MS-S1 - creating tutorials for functions and teaching users how to use buttons the first time that they see them. This is an addition that would be helpful for users, but creating tutorials to use the app is not within the scope of a preliminary version.

3 Use Case Diagram

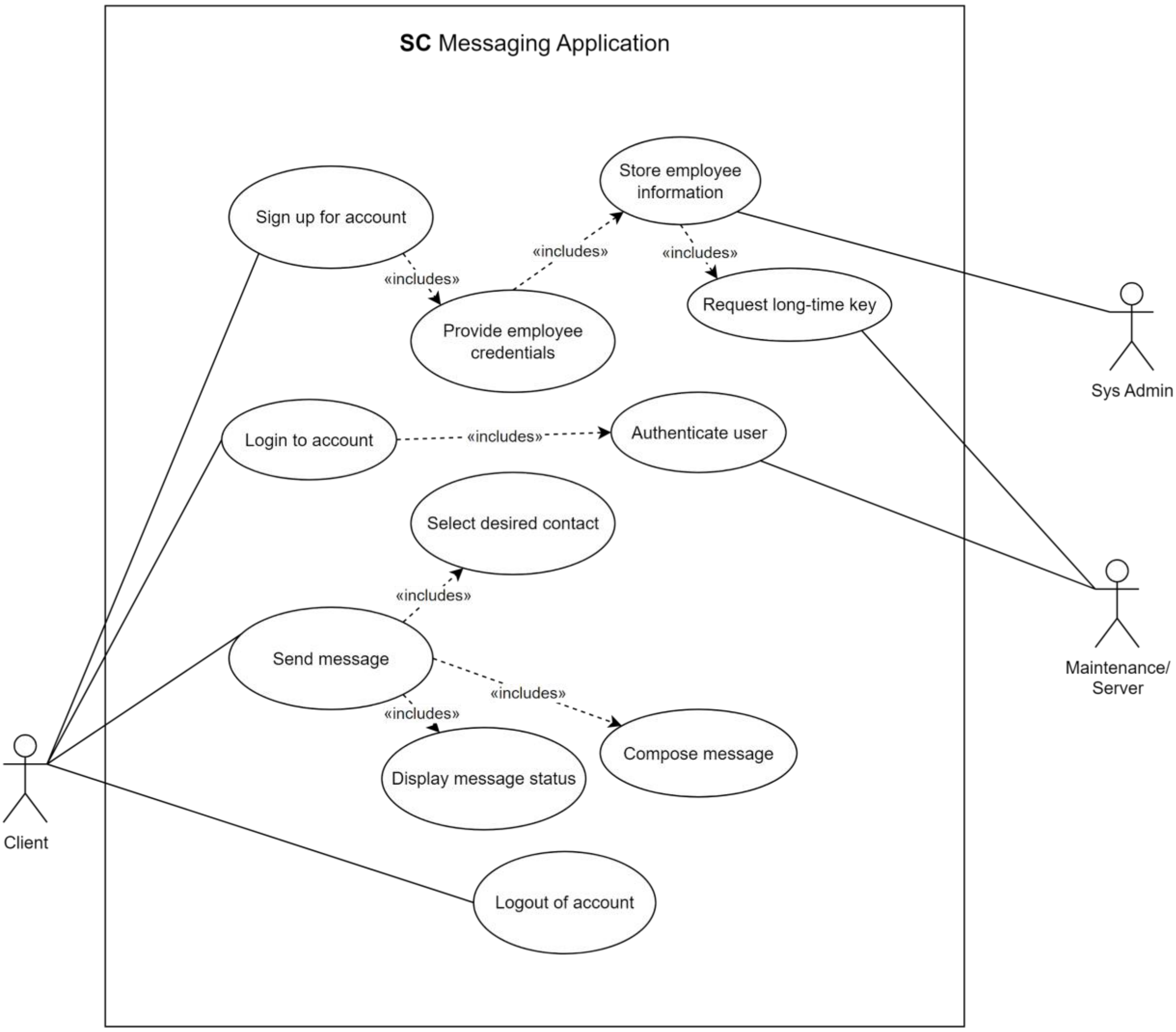

Figure 3. SC Messaging System Use-Case Diagram

4 Highlights of Functional Requirements

The business events we will consider include:

- BE1. Signing up for an account / getting a chatting verification credential
- BE2. Schedule a Meeting
- BE3. Sending a Message
- BE4. Logging Into an Account
- BE5. Logging Out of an Account
- BE6. Closing a Message Thread
- BE7. Requesting a Summary of Recent Messages

The Viewpoints we will consider are:

- VP1. User
- VP2. System Administrator
- VP3. Legal
- VP4. Maintenance/Development
- VP5. Security
- VP6. Funding
- VP7. Business Owner
- VP8. Human Resources

Business Events:

BE1. Signing up for an account / getting a chatting verification credential

Pre-condition: User has no account and wants to sign up for an account.

VP1. User #1

Main Success Scenario

1. User opens up SC software on their phone.
2. User chooses to sign up for an new account.
3. System asks the user to input information they want to use for sign up.
4. User input information.
5. System validates information against the internal database and confirms that the user inputs valid information and no account has been signed up by that information.
6. System creates a new account for the user and creates a verification credential for the user, associated with their ID.
7. System indicates to the user that the user's verification credential has been associated with their account.

Secondary Scenario

5i. System validates information against the internal database and finds the information is not valid or there is an existing account.

5i.1 System validates information against the internal database and finds the information is not valid or there is an existing account.

5i.2 System cannot create a new account for the user and indicate to the user that the sign up failed. [Fail]

VP2. System admin #2

1. User asks the system admin to help them sign up.
2. Admin requests to add a new employee to the internal database.
3. System requests that the admin provides the user’s credentials which the user can use to verify themselves when signing up.
4. Admin provides credentials to the system, including the employee’s ID.
5. System confirms that the credentials do not overlap with any existing employees, and informs the admin that the employee can now register for an account.

Secondary Scenario

5i. If there is overlap, the system admin will help the user initialize their account and reset the password.

VP3. Legal #3

1. Legal team requests to view system configuration to ensure data is properly protected and stored and all rules and regulations are adhered to.[Out of scope]

VP4. Maintenance/Development #4

1. Maintenance requests to see the status of the database and ensure all tables are up to date, have no issues regarding incorrect or missing data, and that the on-prem server is running with no unexpected outages. [Out of scope]

VP5. Security #5

1. Security team requests to see logs to ensure there have been no data breaches. [Out of scope]

VP6. Funding #6

1. Funding requests to see the amount of people signed up in the system so they can compare it to the total number of employees and know if maintaining the system is something they want to keep doing depending on if it is being used or not. [Out of scope]

VP7. Business owner #7

1. Owner requests to see logs and reports of use, consolidating information given to funding, security, maintenance, and legal, allowing them to have a high level view of how the system is helping their company.[Out of scope]

VP8. Human Resources #8

1. Human Resources request information on how many users are registered in the system.
2. System provides a list of employee IDs for those registered.

3. Human Resources thank the system and use the results to warn unregistered users that their continued employment with the company is contingent on having an account.

Global Scenario:

Pre-condition: User has no account and wants to sign up for an account.

Main Success Scenario

1. User opens up SC software on their phone.
2. User chooses to sign up for an new account.
3. System asks the user to input information they want to use for sign up.
4. User input information.
5. System validates information against the internal database and confirms that the user inputs valid information and no account has been signed up by that information.
6. System creates a new account for the user and creates a verification credential for the user, associated with their ID.
7. System indicates to the user that the user's verification credential has been associated with their account.
8. Human Resources request information on how many users are registered in the system.
9. System provides a list of employee IDs for those registered.
10. Human Resources thank the system and use the results to warn unregistered users that their continued employment with the company is contingent on having an account.

Secondary Scenario:

5i. System validates information against the internal database and finds the information is not valid or there is an existing account.

5i.1 System validates information against the internal database and finds the information is not valid or there is an existing account.

5i.2 System cannot create a new account for the user and indicate to the user that the sign up failed. [Fail]

BE2. Schedule a Meeting

Pre-condition: The user is an employee of the company and has already logged in on their phone.

VP1. User #1

Main Success Scenario

1. The user opens the application on their phone.
2. System shows the home page.
3. User chooses to schedule meetings.
4. System gives the user options to choose from (Schedule a new meeting, canceling a meeting, join in a meeting, change a meeting etc.)
5. User chooses to schedule a new meeting.
6. System asks for information including meeting time and asks the user to set a password.

7. User input information.
8. User gets the meeting ID, meeting link.
9. User sends invitations to related colleagues. [Loop to 3]

Secondary Scenario:

5i. User chooses to cancel a meeting.
 5i.1 User chooses to cancel a meeting
 5i.2 System asks the user for the existing meeting ID and password if any.
 5i.3 User inputs info
 5i.4 System prompts user to confirm deletion of meeting
 5i.5 User agrees to cancel the meeting. [Loop to 3.]

5ii. User chooses to join in a meeting.
 5ii.1 User chooses to join in a meeting
 5ii.2 System send meeting notification lists to users
 5ii.3 User chooses a meeting to join in.
 5ii.4 System prompts the user to go to an external website [Loop to 3.]

5iii. User chooses to change a meeting.
 5ii.1 User chooses to change a meeting
 5ii.2 System asks the user for information including the existing meeting ID and password if any. And ask for the new meeting time.
 5ii.3 User inputs information.
 5ii.4 System confirms with the user to change the meeting to a new time.
 5ii.5 User agrees to change the meeting. [Loop to 3.]

VP2. System Admin #2

VP3. Legal #3

N/A

VP4. Maintenance/Development #4

4i.1. Tells the system that when in maintenance, there should be an announcement for users.

VP5. Security #5

N/A

VP6. Funding #6

N/A

VP7. Business Owner #7

1. Business Owners don’t want to hold a meeting for employees any more
   1.1. Business Owners don't want to hold a meeting for employees any more, and users have no need to schedule meetings. Failure.

VP8. Human Resources / Enforcers #8

1. The Human Resource department requests that the system provides a list of colleagues who should attend the meeting.

Global Scenario:

Pre-condition: The user is an employee of the company and has already logged in on their phone.

Main Success Scenario

1. The user opens the application on their phone.
2. System shows the home page.
3. User chooses to schedule meetings.
4. System gives the user options to choose from (Schedule a new meeting, canceling a meeting, join in a meeting, change a meeting etc.)
5. User chooses to schedule a new meeting.
6. System asks for information including meeting time and asks the user to set a password.
7. User input information.
8. User gets the meeting ID, meeting link.
9. User sends invitations to related colleagues. [Loop to 3.]

Secondary Scenario:

1i. Business Owners want to hold a meeting for employees

1i.1 Business Owners want to hold a meeting for employees and ask one of their employees to schedule it.

1i. Business Owners don’t want to hold a meeting for employees

1ii.1 Business Owners don't want to hold a meeting for employees. Failure.

1iii. The Human Resource department requests that the system provides a list of colleagues who should attend the meeting.

4i.1. Tells the system that when in maintenance, there should be an announcement for users.

5i. User chooses to cancel a meeting.

5i.1User chooses to cancel a meeting

5i.2System asks the user for the existing meeting ID and password if any.

5i.3User inputs info

5i.4System prompts user to confirm deletion of meeting

5i.5User agrees to cancel the meeting. [Loop to 3.]

5ii. User chooses to join in a meeting.

5ii.1 User chooses to join in a meeting

5ii.2 System send meeting notification lists to users

5ii.3 User chooses a meeting to join in.

5ii.4 System prompts the user to go to an external website [Loop to 3.]

5iii. User chooses to change a meeting.

5iii.1 User chooses to change a meeting

5iii.2 System asks the user for information including the existing meeting ID and password if any. And ask for the new meeting time.

5iii.3 User inputs information.

5iii.4 System confirms with the user to change the meeting to a new time.

5iii.5 User agrees to change the meeting. [Loop to 3.]

BE3. Sending a Message

Pre-condition: The user is already an employee of the company, has an account in the chat application, and is successfully logged into their account.

VP1. User #1

Main Success Scenario

1. User chooses the desired contact to whom they will send a chat message.
2. System verifies that the message recipient is still authorized to receive messages from the user and establishes a secure communication channel [Jump to VP5.1].
3. User is presented with a chat log with the selected contact, if it exists, with the option to type a chat message.
4. User composes a chat message and requests to send it to the selected contact.
5. System transmits message from user to recipient.
6. System displays to the user a successful message delivery indicator [Jump to VP3.2].

Secondary Scenario:

3i. User fails to interact with the system for 28 minutes, so the system issues a session termination warning if no actions are taken within 2 minutes.
   3i.1 User interacts with the system [Jump to VP1.3].
   3i.2 User fails to interact with the system, so the system terminates the chat session.

6i. System displays to the user a failed message delivery indicator.
   6i.1. User chooses to delete the failed message.
   6i.2. User chooses to report unexpected message delivery failure [Jump to VP4.1].
   6i.3. User attempts to resend the failed message [Jump to VP1.4].

VP2. System Administrator #2

Suspicious Behavior Response Scenario [Out of scope]

1i. System administrator manually reviews the potentially suspicious behavior [Out of scope].
   1i.1 System administrator deems suspicious user behavior as harmless.
   1i.2 System administrator deems suspicious user behavior to be in violation of company policy [Jump to VP3.1].

VP3. Legal #3

Suspicious Behavior Response Scenario [Out of scope]

1i. Legal team reviews actions and actors involved [Out of scope].
   1i.1 Actions of the user abide by company policy, no further action occurs.
   1i.2 Actions of the user violate company policy, so discretionary actions are carried out [Jump to VP8.1].

2i. System displays to the user a successful message delivery indicator.
   2i.1 Message is logged for internal/external auditing should there be a breach of company policy [Extreme boot-licker bourgeoisie feature] [Out of scope].

VP4. Maintenance/Development #4

Failed Message Delivery Response Scenario [Out of scope]

1i. User chooses to report unexpected message delivery failure.
   - 1i.1 Message delivery failure occurred due to user-sided failure, e.g., network connection issues, discard report and inform the user.
   - 1i.2 Message delivery failure occurred for other reasons, e.g., program failure, the user is prompted to choose between uploading a logfile of actions that lead to the failure with or without a description [Jump to VP1.3] [Out of scope].

VP5. Security #5

Suspicious Behavior Response Scenario [Out of scope]

1i. System identifies that the message recipient is authorized to receive messages from the user [Jump to VP1.3].

2i. System identifies that the message recipient is *not* authorized to receive messages from the user.
   - 2i.1 System alerts the system administrator of potentially suspicious behavior [Jump to VP2.1].

VP6. Funding #6

N/A

VP7. Business Owner #7

N/A

VP8. Human Resources #8

Suspicious Behavior Response Scenario [Out of scope]

1i. Actions of the user violate company policy, discretionary actions are carried out.
   - 1i.1 User receives security training.
   - 1i.2 User is fired.

Global Scenario:

Pre-condition: The user is already an employee of the company, has an account in the chat application, and is successfully logged into their account.

Main Success Scenario

1. User chooses the desired contact to whom they will send a chat message.
2. System verifies that the message recipient is still authorized to receive messages from the user and establishes a secure communication channel.
3. User is presented with a chat log with the selected contact, if it exists, with the option to type a chat message.
4. User composes a chat message and requests to send it to the selected contact.
5. System transmits message from user to recipient.

6. System displays to the user a successful message delivery indicator [Jump to S1].

Secondary Scenario:

- 2i. System identifies that the message recipient is authorized to receive messages from the user [Jump to 3].
- 2ii. System identifies that the message recipient is not authorized to receive messages from the user.
  - 2ii.1 System alerts the system administrator of potentially suspicious behavior.
  - 2ii.2 System administrator manually reviews the potentially suspicious behavior [Out of scope].
    - 2ii.2i.1 System administrator deems suspicious user behavior as harmless.
    - 2ii.2i.2 System administrator deems suspicious user behavior to be in violation of company policy [Jump to S2].
- 3i. User fails to interact with the system for 28 minutes, so the system issues a session termination warning if no actions are taken within 2 minutes.
  - 3i.1 User interacts with the system [Jump to 3].
  - 3i.2 User fails to interact with the system, so the system terminates the chat session.
- 6i. System displays to the user a failed message delivery indicator.
  - 6i.1. User chooses to delete the failed message.
  - 6i.2. User chooses to report unexpected message delivery failure [Jump to S3].
  - 6i.3. User attempts to resend the failed message [Jump to 4].

Suspicious Behavior Response Scenario [Out of scope]

- S1. System displays to the user a successful message delivery indicator.
  - S1.2. Message is logged for internal/external auditing should there be a breach of company policy [Extreme boot-licker bourgeoisie feature] [Out of scope].
- S2. Legal team reviews actions and actors involved [Out of scope].
  - S2.1. Actions of the user abide by company policy, no further action occurs.
  - S2.2. Actions of the user violate company policy, so discretionary actions are carried out [Jump to S4].
- S3. User chooses to report unexpected message delivery failure.
  - S3.1. Message delivery failure occurred due to user-sided failure, e.g., network connection issues, discard report and inform the user.
  - S3.2. Message delivery failure occurred for other reasons, e.g., program failure, the user is prompted to choose between uploading a logfile of actions that lead to the failure with or without a description [Jump to 3] [Out of scope].
- S4. Actions of the user violate company policy, discretionary actions are carried out.
  - S4.1. User receives security training.
  - S4.2. User is fired.

BE4. Logging Into an Account

Pre-condition: The user is already an employee of the company, has an account in the chat application.

VP1. User #1

1. User launches the chat application
2. Server loads loading page
3. User enters log-in information
4. Server authenticates log-in information

VP2. System Administrator #2

1. System alerts the system administrator of potentially suspicious behavior [Out of scope].
2. System administrator manually reviews the potentially suspicious behavior [Out of scope].
3. System administrator deems suspicious user behavior as harmless.
4. System administrator deems suspicious user behavior to be in violation of company policy [Jump to VP3.1].

VP3. Legal #3

N/A

VP4. Maintenance/Development #4

1. Maintenance is alerted if logging in issues persist.

VP5. Security #5

N/A

VP6. Funding #6

N/A

VP7. Business Owner #7

N/A

VP8. Human Resources #8

N/A

Global Scenario:

Pre-condition: The user is already an employee of the company, has an account in the chat application.

Main Success Scenario

1. User opens the application
2. System displays landing page with login fields
3. User enters log-in information
4. System authenticates the user information

Secondary Scenario:

4i. If the authentication is successful, the enter is logged in and is directed to their messages

4ii. If the authentication fails, the user is redirected to the landing page and an error message appears

4ii.1 Repeated failures will cause the notification of the system administrator

BE5. Logging Out of an Account

Pre-condition: The user is already an employee of the company, has an account in the chat application and is logged into the application.

VP1. User #1

1. User logs out of the application
2. System redirected user to landing page

VP2. System Administrator #2

1. The system administrator can receive information about what users are logged out.

VP2. Legal #3

N/A

VP3. Maintenance/Development #4

1. Maintenance is alerted if logout issues persist.

VP4. Security #4

N/A

VP5. Funding #5

N/A

VP6. Business Owner #6

N/A

VP7. Human Resources #7

N/A

Global Scenario:

Pre-condition: The user is already an employee of the company, has an account in the chat application and is logged into the application.

Main Success Scenario

1. User logs out of the application
2. System redirected user to landing page
3. System updates information of logout for user that the system administrator can access

Secondary Scenario:

3i. The system administrator can receive information about what users are logged out.
3ii. Maintenance is alerted if logout issues persist.

BE6. Closing a message thread

Pre-condition: The user is already an employee of the company, and has an account in the chat application. The user is signed into the application.

Main Success Scenario

1. The user navigates to the message thread they wish to close.
2. User selects the option to close the message thread.
3. System prompts the user for confirmation to close the message thread.
4. User confirms the action.
5. System removes the message thread from the user's view.

Secondary Scenario

1i. User is inactive for too long (30 minutes)

1i.1 User is inactive for too long (30 minutes)
1i.2 System gives user a warning that if no messages are sent, the session will be terminated
1i.3 User continues to be inactive
1i.4 System terminates the session and invalidates the session key

2i. The user initiates the deletion of their chat with a particular user.
2i.1 The user initiates the deletion of their chat with a particular user.
2i.2 Upon confirmation, all data associated with the chat is wiped from the user's accessible records.
2i.3 Access to the deleted data is restricted to system administrators for a specified period, typically 90 days, before automatic recycling.

VP7. Human Resources #7
N/A

VP2. System Administrator #2
N/A

VP3. Legal #3
N/A

VP4. Maintenance/Development #4
N/A

VP5. Security #5
N/A

VP6. Funding #6
N/A

VP7. Business Owner #7

N/A

VP8. Human Resources #8

N/A

Global Scenario:

Pre-condition: The user is already an employee of the company, and has an account in the chat application. The user is signed into the application.

Main Success Scenario

1. User selects the option to close the message thread.
2. System prompts the user for confirmation to close the message thread.
3. User confirms the action.
4. System removes the message thread from the user's view.

Secondary Scenario:

1i. User is inactive for too long (30 minutes)

- 1i.1 User is inactive for too long (30 minutes)
- 1i.2 System gives user a warning that if no messages are sent, the session will be terminated
- 1i.3 User continues to be inactive
- 1i.4 System terminates the session and invalidates the session key

2i. The user initiates the deletion of their chat with a particular user.

- 2i.1 The user initiates the deletion of their chat with a particular user.
- 2i.2 Upon confirmation, all data associated with the chat is wiped from the user's accessible records.
- 2i.3 Access to the deleted data is restricted to system administrators for a specified period, typically 90 days, before automatic recycling.

BE7. Requesting a summary of recent chat messages

Pre-condition: User has already chatted with colleagues and has chat history which can be summarized.

VP1. User

Main Success Scenario

1. User chooses messages to be summarized.
2. System prompts the user to confirm they want to summarize it with summarization tools.
3. User agrees to use summarization tools.
4. User waits for summarization tools to finish their job.
5. System sends successful summarization back to the user.

Secondary Scenario

1i. User chooses too many messages or chooses pictures/voice messages which cannot be summarized.

 1i.1 User chooses too many messages or chooses pictures/voice messages which cannot be summarized.
 1i.2 Summarize failed, system admin prompts user to choose valid messages.
 1i.3 User chooses messages again.

3i. User does not agree to use the summarization tool. (Fail)

 3i.1 User does not agree to use a summarization tool.
 3i.2 Summary request failed.

5i. Summarize unsuccessfully by summarization tool

 5i.1 Summarize unsuccessfully by summarization tool
 5i.2 System admin prompts the user to request the summary again.

VP2. System Administrator

N/A

VP3. Legal

N/A

VP4. Maintenance/Development

N/A

VP5. Security

5ii. Security requests logs of all messages sent to the summarization tool.
5iii. System provides logs of messages sent.

VP6. Funding

N/A

VP7. Business Owner

N/A

VP8. Human Resources

N/A

Global Scenario:

Pre-condition: User has already chatted with colleagues and has chat history which can be summarized.

Main Success Scenario

1. User chooses messages to be summarized.
2. System prompts the user to confirm they want to summarize it with summarization tools.
3. User agrees to use summarization tools.
4. User waits for summarization tools to finish their job.
5. System sends successful summarization back to the user.

Secondary Scenario:

1i. User chooses too many messages or chooses pictures/voice messages which cannot be summarized.
  1i.1 User chooses too many messages or chooses pictures/voice messages which cannot be summarized.
  1i.2 Summarize failed, system admin prompts user to choose valid messages.
  1i.3 User chooses messages again.
3i. User does not agree to use the summarization tool. (Fail)
  3i.1 User does not agree to use a summarization tool.
  3i.2 3i.2 Summary request failed.
5i. Summarize unsuccessfully by summarization tool
  5i.1 Summarize unsuccessfully by summarization tool
  5i.2 System admin prompts the user to request the summary again.
5ii. Security requests logs of all messages sent to the summarization tool.
5iii. System provides logs of messages sent.

5 Non-Functional Requirements

5.1 Look and Feel Requirements

5.1.1 Appearance Requirements

LF-A1. The system should use an accessible color scheme by using high contrast colors.
Rationale: Adhering to accessibility guidelines accommodates users with diverse needs as high contrast colors make it easier to differentiate components.

LF-A2. The system should use consistent branding elements.
Rationale: Consistency in branding reinforces the organization’s identity and fosters a sense of familiarity among users.

LF-A3. The system should use a minimalist, professional design.
Rationale: This design choice ensures that users can easily navigate through the app and concentrate on the content without distractions.

LF-A4. The system should use visual indicators to communicate the level of security and encryption employed in the communication channels.
Rationale: Clear security indicators help users trust the confidentiality and integrity of their conversations.

5.1.2 Style Requirements

LF-S1. The system should use a design system which standardizes visual elements.
Rationale: Implementing a design system ensures consistency, efficiency, scalability, and brand coherence in the application's visual elements.

LF-S2. The system should be responsive.
Rationale: Ensuring responsiveness across different screen sizes enhances usability and

accessibility by accommodating users on various devices, including smartphones, tablets, and desktops.

5.2 Usability and Humanity Requirements

5.2.1 Ease of Use Requirements

UH-EOU1. The system should teach the user how to use features the first time users see them.
Rationale: Ensuring there is explicit communication so that the user knows how to use every feature allows them to easily use it without any prior knowledge.

UH-EOU2. Buttons with no obvious meaning (eg. An image of a home for the home button is considered obvious, but a clock image could be for a clock, a timer, a stopwatch, etc.) should be labeled.
Rationale: To ensure ease of use for all users, button labels are a necessary addition for users to always know what a button does.

5.2.2 Personalization and Internationalization Requirements

UH-PI1. The system should be able to be downloaded in different countries, and support different languages.
Rationale: We are assuming that the company employs people from different cultural backgrounds with different first languages that they are comfortable with. This will ensure the app can be used by people from different cultures.

UH-PI2. The system should support choices of different color theme modes.
Rationale: This requirement is designed to make sure personalization is satisfied. Giving users choices of appearance and theme allows flexibility on personalization.

5.2.3 Learning Requirements

UH-L1. The system should provide simple tutorials/instructions for users to follow. Users can choose to skip that tutorial. A simple tutorial is a tutorial with less than 5 steps to remember for each item it teaches and has instructions that are less than 50 words per step.
Rationale: This requirement can be helpful when users learn to use the app. It will make the app easier to use and ensure all users have instructions to reference so people of all skill levels and backgrounds can use the app.

UH-L2. The user should be able to begin using the app and send their first message within their first 10 minutes of use.
Rationale: To ensure smooth setup for users and compliance with using **SC**, the layout and features should be intuitive, allowing for users to quickly begin messaging. 10 minutes was chosen due to the simplicity of the system that is expected to be built, and is based on the small amount of features required for the user to send a message, which are simply logging in, finding someone to chat with, and typing a message to send.

5.2.4 Understandability and Politeness Requirements

UH-UP1. All bad words should become stars (*) to avoid impoliteness.
Rationale: This requirement is designed to provide a clean work environment, no workplace-inappropriate words will be allowed. A better communication environment can protect our users.

5.2.5 Accessibility Requirements

UH-A1. The system should support screen readers.
Rationale: We assume that some of the employees might have reading disabilities and will appreciate having a feature that speaks out loud to help them understand both how the app works and also read messages aloud to them.

UH-A2. The system provides color blind mode.
Rationale: We are assuming that some of the employees might be color blind. Providing a color blind mode can make them comfortable when they need to recognize colors.

UH-A3. Convert voice message to text.
Rationale: This will make it easier for people with hearing disability or people who are in noisy environments to check voice messages.

UH-A4. The system shall offer a text magnification option.
Rationale: This feature would aid visually-impaired individuals in viewing texts.

5.3 Performance Requirements

5.3.1 Speed and Latency Requirements

PR-SL1. Messages should be successfully sent to the server and successfully received by the recipient within ≤ 1s delay after the user sends the message from their device [PR-SL1].
Rationale: Ensuring the messages are as fast as possible, we provide an environment with little delay in time response which promotes productivity and no stress from messages not sending.

PR-SL2. The system should mark messages with visual cues to notify users they are sent/received successfully.
Rationale: This will ensure users know their communication status.

5.3.2 Safety-Critical Requirements

N/A

5.3.3 Precision or Accuracy Requirements

PR-PA1. The time shown on scheduled meetings is precise and accurate to exactly 1 minute.

Rationale: To limit confusion and ensure ease of scheduling, users will only be able to schedule meetings up to a precision of 1 minute. Meeting applications such as google calendar use a precision up to a minute as scheduling to the second is unrealistic.

PR-PA2. The system shall display messages' receival time in the chat log to within 1-minute accuracy.
Rationale: To not have any confusion about when messages were sent and received, they must have accurate timestamps. There is no specific standard online for this, but chat applications such as iMessage and Instagram display timestamps accurate to around 1 minute, if not right on the minute. Thus, this internal chat application should have a similar accuracy to achieve this unofficial industry standard.

5.3.4 Reliability and Availability Requirements

PR-RA1. The system shall only have forecasted downtime of an overnight (at most 12-hours long) maintenance every month on a weekend.
Rationale: To maintain integrity in the system and ensure security, it is expected that once a month maintenance will be performed. At most 12 hours is a conservative estimate to ensure there is enough time to complete maintenance. Due to this being a system for a corporate space, we assume that employees are not working on weekends. Maintenance typically is reserved for 12 hours, which is why that number was chosen [PR-RA1]. As mentioned in [MS-M1], we have decided on monthly maintenance, which is why the downtime is every month.

5.3.5 Robustness or Fault-Tolerance Requirements

PR-RFT1. Upon disconnection from the network, the system will automatically try and re-establish connection.
Rationale: Network problems are a possible interruption that could happen to users while using **SC**. By ensuring that any disconnections result in automatic reconnection to the secure chat channel, the system is more robust and reliable, enhancing user experience as well.

5.3.6 Capacity Requirements

PR-C1. The system shall facilitate at least as many employees as there are in the system concurrently.
Rationale: By supporting at least as many employees as there are in the system concurrently, in the chance that all users are on the system at once, no one will experience any delays in work.

5.3.7 Scalability or Extensibility Requirements

PR-SE1. The system should support scaling upwards to accommodate more users.
Rationale: To allow the company to grow without problems arising from an increased user base, the system must allow itself to support new users as time passes.

5.3.8 Longevity Requirements

PR-L1. The system should persist messages for at least 1 year after they were sent.
Rationale: To allow users to go back and view potentially relevant messages that they have sent, they should be persisted for at least 1 year after the date of sending. Inspiration was taken from Apple's iMessage message retention, where the longest amount of time that messages persist is forever, and the second longest is a year. To not overload the system storage as well as for safety reasons, messages persisting forever is not ideal. Deleting messages after 1 year ensures irrelevant chats are erased but users can still reference potentially relevant information from the past year whenever they want.

5.4 Operational and Environmental Requirements

5.4.1 Expected Physical Environment

OE-EPE1. The system is expected to run on an android device.
Rationale: The company that has requested **SC** requires it for android devices.

5.4.2 Requirements for Interfacing with Adjacent Systems

OE-IA1. The system must be able to send and receive messages with a LLM.
Rationale: In order to allow for chat summarization, the system must interface with some connection.

5.4.3 Productization Requirements

N/A

5.4.4 Release Requirements

OE-R1. The system must be compatible with Android 10.0 or above
Rationale: With Android 14 being the most recent as of February 9, 2024, allowing for up to 4 versions ago for releases should ensure that all employees are able to use the system.

5.5 Maintainability and Support Requirements

5.5.1 Maintenance Requirements

MS-M1. The system should be regularly maintained and checked for bugs on every OS update that the hosting device receives. Regular maintenance is defined as monthly maintenance, in addition to those for every OS update.
Rationale: OS updates can cause major breaks in software and also patch security faults, therefore to ensure the integrity of the system, the system must be updated as the device OS is. For monthly maintenance, this was chosen because it is a common regular time frame, and the system is not safety critical enough to require weekly maintenance. [MS-M1]

5.5.2 Supportability Requirements

MS-S1. The system should contain in-app tutorials on basic functions of the app.
Rationale: Users must have a way to easily refresh themselves on the functionality of the app, therefore ensuring they can always feel comfortable and supported using it. The tutorials must be in-app to help with ease of access and allow for them to be walked through the tutorials dynamically.

5.5.3 Adaptability Requirements

MS-A1. The system must always be able to run on the most current Android version available for Android devices within a day of release.
Rationale: As updates can be frequent for mobile devices to ensure integrity, the system must adapt to these updates to ensure users experience no lag time where they are unable to use the app.

5.6 Security Requirements

5.6.1 Access Requirements

SR-AC1. The user-interface portion of the system should only be accessible to authenticated individuals by the company.
Rationale: To prevent security breaches, the system must not be accessible to outsiders.

SR-AC2. The system must support a form of authentication that uses company specific information.
Rationale: By using company specific information, only individuals of the company have a chance to authenticate.

SR-AC3. The back-end of the system must only be accessible to system admins and those they give permission to.
Rationale: The back-end will have private information that must be secure, and thus should only be accessible to those with proper security clearance.

SR-AC4. The system should encrypt user information, passwords, and chat logs end to end.
Rationale: The database should not contain any information that is confidential to either the user or the business in case of a security breach.

5.0.1 Integrity Requirements

SR-INT1. All chat logs and server communication should be encrypted.
Rationale: As security has been deemed the largest concern due to potential corporate espionage, encryption is strictly necessary for maintaining security. Other online apps such as WhatsApp also encrypt data, and they are used for regular communication [SR-INT1].

5.0.2 Privacy Requirements

SR-P1. The system must prevent any leakage of personal identifiable information (PII) during communication.

Rationale: Employee personal information must be protected and secure to adhere to privacy regulations.

5.0.3 Audit Requirements

SR-AU1. The system should maintain a history of changes made to all aspects of the system.
Rationale: Auditing will likely include viewing the progress of the system over time, meaning there could be consequences to not maintaining a history.

5.0.4 Immunity Requirements

SR-IM1. The system must not accept unexpected input.
Rationale: This prevents attacks like SQL injection.

5.1 Cultural and Political Requirements

5.1.1 Cultural Requirements

CP-C1. The system should not contain any offensive or hurtful languages to any existing cultures.
Rationale: To ensure a diverse set of employees can use the system without worry, no cultures should have any hurtful language targeted towards them.

5.1.2 Political Requirements

CP-P1. The system must not promote any political ideologies.
Rationale: Employees could get offended by having ideologies forced upon them, especially when political beliefs are a sensitive topic to some.

5.2 Legal Requirements

5.2.1 Compliance Requirements

LR-COMP1. All personal information collected on the employees must be protected.
Rationale: This follows PIPEDA (Personal Information Protection and Electronic Documents Act) Fair Information Principle 1 - Accountability [LR-COMP1]

5.2.2 Standards Requirements

LR-STD1. The app shall have touch targets that are at least 48dp in size.
Rationale: This is a standard based on the android core app quality page [LR-STD1].

LR-STD2. The app's text and foreground content should maintain a high enough color contrast ratio with its background:

- 3.0:1 for large text / graphics
- 4.5:1 for small text (text smaller than 18pt, or if the text is bold and smaller than 14pt)

Rationale: This is a standard based on the android core app quality page [LR-STD1].

LR-STD3. The system shall implement security controls to protect confidentiality, integrity and availability of IT assets against threat agent capabilities, natural hazards or accidental events.
Rationale: This is a standard based on the Canadian Centre for Cyber Security's "User authentication guidance for information technology systems (ITSP.30.031 v3)" [LR-STD3].

6 Innovative Feature

The innovative feature that we came up with is meeting scheduling. Meeting scheduling would allow the users to schedule in person or online meetings and keep track of them on the calendar and have optional push notifications to the user's device that could contain the meeting link if provided by the user who created the meeting initially.

Another innovative feature is message summarization using an existing AI large language model. This feature could be useful for users who want to get a summarization of a large message if they are on the go and want to stay up to date with the company's current status. This feature would be optional and can be disabled in the app settings.

7 A Division of Labour

Include a Division of Labour sheet which indicates the contributions of each team member. This sheet must be signed by all team members.

Kyle Hagerman

[redacted]

- Completed BE1
- Added session key information and secondary scenario to BE3 VP1
- Added BE1 and session key info from BE3 to use case diagram
- Went through all non functional requirements (NFRs) with the team, wrote about 30-35% of NFRs, including some references
- 2.3 User Characteristics
- 2.4 Constraints
- 2.6 Apportioning of Requirements
- Added to 1.1 Purpose
- Reviewed entire document with the team before submitting
- Modified NFRs to have more sources where numbers were used, as well as explanations when no sources existed, and remove ambiguity of wording

Michael Breau

MB

- Completed BE4 and BE5
- Completed SR-AC4, CP-C2
- Innovative Feature Section (6)
- Overview (1.5)
- Assumptions and Dependencies (2.5)
- Added BE4, BE5 info to use case diagram

Zongcheng Li

Z.L.

- Introduction text (1)
- Purpose(1.1)
- Product Functions (2.2)
- Participate in teamwork of drawing Use Case Diagram (3)
- Highlights of Functional Requirements lists of B.E. and V.P. (4)
- B.E.2 Scheduling a meeting (4 B.E.2)
- B.E.7 Requesting a summary of recent chat messages (4 B.E.7)
- Write part of non-functional requirements (5.2.2-5.2.5)

Jay Sharma

J.S

- Completed Scope (1.2)
- Completed BE6
- Went through all non functional requirements (NFRs) with the team, wrote about 30-35% of NFRs
- Participate in teamwork of drawing Use Case Diagram (3)
- Reviewed entire document with the team before submitting

Ahmed Al-Hayali

- 2.1 Product Perspective
- 3 Use Case Diagram
- 4 Business Event 3
- Contribution in group discussions when discussing NFRs
- Contribution in group discussions when reviewing the document

A.A.