Security Policy	Confidentiality, Integrity, and Availability					
security Requirements	**Security mechanisms (List down for your application)**	**Remarks on why you considered these requirements? (in a brief)**	**Supplement requirements for your application** **(user story/Abuse case)**	**Risk identification/Threat Assessment (at least one risk identification/abuse case)**	**appropriate Security Controls**	**Tick ✔if you have applied the given security controls as suggested in the left column**
Authentication	Registered phone number	For granting only the users in this house can access the smart home, we need to register the accounts with their phone number	*Goal*: The system ensures that the phone numbers exist. *Requirement*:To register the application, the users should use their phone numbers. *User story*: “As a user, I can enter my phone number to register. *Abuse case*: “As an attacker, I can enter a virtual phone number to register.”	1. You enter a wrong phone number more than 3 times. 2. You enter the correct phone number but fail to enter the right passcode. 3. The user enters a phone number which is not the specified format.		
	Password checking	For users to use the app and access their profiles, they need to authenticate with a pin code / password to prevent unauthorized people from accessing the app through the phone of one of the household members	*Goal*: The system verifies that there are no default passwords used by the application or any of its components. *Requirement*: To access the application, one should require authentication.	1. You enter a wrong password more than 3 times. 2. You enter a default password. 3. The length of the password is less than 8 digits.		

			User story: “As a user, I can sign in the application by using my username/phone number and password” *Abuse case*: As an attacker, I can enter the default passwords to access the application.			
	Token system	When users want to register an account or forget the password, we need to use the token to authenticate.	*Goal*: The system ensures that the SMS code is not simple. *Requirement*: The system sends an SMS code to the user that they can use to sign in *User story*: “As a user, I can enter my phone number and then enter the code sent to me by the application through SMS to access it. *Abuse case*: “As an attacker, I can enter the simple and stupid SMS code to register an account.	1. The token is too simple, such as 0000,1234 etc. 2. You enter a wrong SMS token more than three times.		
	Biometric authentication (fingerprint or face recognition)	For some advanced authentication features (Optional; could be used for e.g. adding new users or accessing certain sensitive settings)	*Goal*: The system verifies that the fingerprints and facial data entered are not blurred. *Requirement*: To access the application without password, the user should use his/her face to authenticate. *User story*: As a user, I want to access the application by fingerprint or face recognition. *Abuse story*: As an attacker,	1. You enter wrong biometric data more than 3 times. 2. The biometric data are blurred.		

			I can enter the application by using the photo or model.			
Authorization	Role-based authorization	The admin can register new members and change the settings, others can only control the different smart home components.	*Goal*: The system requires biometric data before the admin can change settings *Requirement*: Regular users can only access the components of the smart system whereas admins can access all settings as well *User story*: “As an admin, I can change all settings of the smart home system”. *Abuse story*: “As an attacker, I get access to all settings if I manage to get into the admin account”	1. You try to perform an operation to which you’re not authorized twice in a row.		
Audit	Protection of log files	To prevent unauthorized users from getting access to personal information through the log files	*Goal*: The system ensures that the password used for accessing the log files is not the same as the password the admin uses for their account in the app *Requirement*: The admin can access the protected log files with a password *User story*: “As an admin, I can enter a password to get access to the log files” *Abuse story*: “As an attacker, I can access to all log files if I get hold of the admin password”	1. You try to open a log file without the proper permissions		
	Encoding of sensitive data (personal identifiable	To prevent people from getting access to this	*Goal*: The system uses hashing to make it harder for	1. You request sensitive data from the server to		

	information, passwords, phone numbers, etc)	sensitive data in case of a data breach	attackers to decipher the encoded data by brute force *Requirement*: The system encodes sensitive user data to protect it in case of an attack *User story*: “As a user, I can safely enter my data in the app because I know it will be encoded” *Abuse story*: “As an attacker, I can use brute force to decipher the encrypted data”	which you do not have access		