1. Test Plan

1.1. Introduction

1.1.1. Purpose

This test plan describes the testing approach and overall framework that will drive the testing of the *Home Surveillance System*.

The plan identify the items to be tested, the features to be tested, the types of testing to be performed, the personnel responsible for testing, the resources and schedule required to complete testing, and the risks associated with the plan.

1.1.2. Project Overview

The Home Surveillance System aims to provide basic security and safety functions. It is capable of alerting the user in case of undesirable activities, such as theft, intrusion, natural hazards, etc.

1.2. Environmental Needs

The following hardware is neccessary to perform complete testing

1. Main Wireless Box, containing the central processor.
2. Sensors, activated and connected to the system
3. Two Control panels
4. A connected mobile device, to check notification systems, as well as check web interface.
5. A dedicated PC having an internet connection, and running Windows 7/10. Must have 4GB RAM, and 20GB disk space.
6. A dedicated Server: Microsoft SQL Server (2012/2014/2016/2017/2019)

1.3. Scope

The following features are tested in this document.

1.3.1. Login/Logout Functionality

Allowing User to login into and logout of the system, as well as additional related functionality, such as checking password strength, changing passwords, logging out automatically after inactivity, etc.

1.3.2. User Interface Functionality

Allows user to access previous recorded video footage, toggle sensors, view current surveillance zone, as well as locate all sensors and cameras currently in the house

1.3.3. Communication Modules

Allows the system to Send notifications to the User's Mobile Device, alert Specific Authorities in cases of emergency, as well as send log files to the security company

1.3.4. System Testing

Tests the combined system response to multiple scenarios.

1.4. Out of Scope

The following features are considered out of scope for this testing document.

1.4.1. Sensors and other Hardware testing

Checking that the sensors respond correctly to their triggers, and return correct output.

1.4.2. Security

The wireless communication between all different components of the system must be encrypted, according to the specifications of the SRS.

1.4.3. Scalability

The software should be capable of supporting a large number of users to a suitable degree.

1.5. Procedure

Most of the User Interface is tested with the help of Selenium.

The Communication module is tested by test files written in native code.

1.6. Test Strategy

The test strategy consists of a series of different tests that will aim to cover the entire home surveillance system.

The primary purpose of these tests is to uncover the systems limitations and measure its full capabilities. A list of the various planned tests and a brief explanation follows below.

1.6.1. System Test

The System tests will focus on the behavior of the home surveillance system, and will test the integrated system against multiple User scenarios, and verify it meets the specifications provided in the SRS.

1.6.2. Performance Test

Performance test will be conducted to ensure that system response times meet user expectations, and do not exceed the performance criteria specified in the SRS.

Stress Testing will be performed to measure the response times when under heavy load..

1.6.3. Security Test

Security Tests will verify that unauthorized users will not have access to any confidential data.

1.6.4. Automated Test

A suite of automated tests will be developed to test the basic functionality of the home surveillance system and perform regression testing on areas of the systems that previously had critical/major defects.

The idea is to use automation in order to emulate multiple users all of which are executing different user scenarios

1.6.5. User Acceptance Test

Once the system is ready for implementation, User Acceptance Testing is performed.

This is to confirm that the system is developed according to the specified user requirements and is ready for operational use.

1.7. Risk Analysis

Risk is assigned on the basis of the level of impact the given test's outcome has on the project

Risk	Probability
High	Must be solved *immediately*
Medium	Must be solved before declaring testing complete
Low	Not of high priority, can use alternative solutions instead

1.8. Exit Criteria

If any defects are found which seriously impact the test progress, then the Testing team may decide to suspend testing.

Possible Criteria which justify test suspension are: - Unavailable Environmental Needs according to schedule. - Critical defects in Source code, which limits testing progress.

If testing is suspended, resumption will only occur when the problem(s) that caused the suspension has been resolved.

If the suspension defect is considered *critical*, it must be verified by the Testing Team before resumption

2. Unit Tests - Test Scenarios

2.1. User Interface Login Testing

This stage of testing determines if a user can access their dashboard given they have their user-id and password.

As the SRS does not mention any method of creating or deleting an account, it is assumed that account creation and deletion is handled by contacting the company at the moment of purchase

2.1.1. Browser / Control Panel Functionality

The User Interface should work on the given web browsers, i.e. Internet Explorer v11 and Chrome v89, The User Panel should also work on the Control Panels itself.

Functionality on previous versions and/or other web browsers is not of immediate priority.

Risk: High

Pre-Condition: None

Steps: Open the Web Interface on the Browser

Test Cases

Test Case	Test Inputs	Expected Result	Post condition
Open on Internet Explorer v>=11 on a PC	Interface URL	Successful	The User Interface is visible and interactive
Open on Internet Explorer v>=11 on a Mobile	Interface URL	Successful	The User Interface is visible, interactive and responsive
Open on Google Chrome v>=89 on a PC	Interface URL	Successful	The User Interface is visible and interactive
Open on Google Chrome v>=89 on a Mobile	Interface URL	Successful	The User Interface is visible, interactive and responsive
Open on Control Panel	None	Successful	The User Interface is visible, interactive and responsive

2.1.2. Check Password Strength

This module is needed to check the strength of the password, when 1. Creating the account, OR 2. Changing the password.

The SRS specifies that the password must contain a combination of letters, numbers and special characters. We assume that atleast one number, atleast one letter, and one special character is required We also assume that passwords must have a minimum length of 6, for security purposes.

The exact values may change later, as per the wishes of the Dev Team.

Risk: Medium

Pre-Condition: None

Steps:

1. Enter password as input to module.
2. Run module.

Test Case	Test Inputs	Expected Result	Post condition
Password contains 6 character combination of letters, numbers and special characters	Password	Successful	None
Password contains 5 character combination of letters, numbers and special characters	Password	Failed	Error Message "Password too Short"
Password contains 6 character combination without special characters	Password	Failed	Error Message "No special characters in password"
Password contains 6 character combination without numbers	Password	Failed	Error Message "No numbers in password"

Test Case	Test Inputs	Expected Result	Post condition
Password contains 6 character combination without letters	Password	Failed	Error Message "No letters in password"

2.1.3. Login into the system

Allows the User to Login into the system

Risk: High

Pre-Condition: User must have a valid account user-id and password.

Steps:

1. Click Menu
2. Enter user-id
3. Enter password
4. Click "Login" Button

Test Cases

Test Case	Test Inputs	Expected Result	Post condition
Enter Valid User-id and Valid Password	Valid Username Valid Password	Successful Login	Get Access to Main Menu
Enter Valid User-id and Invalid Password	Valid Username Invalid Password	Login Failed	Return to Login Popup
Enter Invalid User-id and Valid Password	Invalid Username Valid Password	Login Failed	Return to Login Popup

2.1.4. Block Interface if 5 incorrect account entry attempts

After 5 incorrect entry attempts, the user interface must be blocked, and a log is sent to the security company, as well as the homeowner.

Risk: High

Pre-Condition:

1. User must have valid account user-id and password
2. User must have already attempted entry 4 times, and have failed.

Steps: Same as Login into System

Test Case	Test Inputs	Expected Result	Post condition
Enter Valid User-id and Valid Password	Valid Username Valid Password	Successful Login	Get Access to Main Menu
Enter Valid User-id and Invalid Password	Valid Username Invalid Password	Login Failed	Block Interface for 30 minutes. Send log to company and homeowner.
Enter Invalid User-id and Valid Password	Invalid Username Valid Password	Login Failed	Block Interface for 30 minutes. Send log to company and homeowner.
Enter Invalid User-id and Invalid Password	Invalid Username Invalid Password	Login Failed	Block Interface for 30 minutes. Send log to company and homeowner.

2.1.5. Check Failed Login Block Timeout is 30 minutes.

If the Login Page has been blocked due to multiple failed login attempts, then the timeout period must be 30 minutes.

Risk: Medium

Pre-condition:

1. User must have blocked the interface by providing invalid user-id / password.

Steps: Same as Login into System

Test Case	Test Inputs	Expected Result	Post condition

Test Case	Test Inputs	Expected Result	Post condition
Login attempt after 20 minutes	User-id, password	Login Page does not allow you to enter credentials	None
Login attempt after 30 minutes	User-id, password	Login Page allows you to enter credentials	User can attempt to Login
Login attempt after 40 minutes	User-id, password	Login Page allows you to enter credentials	User can attempt to Login

2.1.6. Logout after 30 minute Inactivity

If the user has been inactive for 30 minutes or more, then the user should be logged out of the interface.

Risk: High

Pre-conditions:

1. User must be logged in into the system

Steps:

1. User must leave the system inactive for certain period of time.

Test Case	Test Inputs	Expected Result	Post condition
Let User be inactive for 20 minutes.	None	Dashboard is still active	None
Let User be inactive for 30 minutes.	None	User is logged out.	User redirected to Login Page
Let User be inactive for 40 minutes.	None	User is logged out.	User redirected to Login Page

2.1.7. Single Control Panel Enabled.

The software only allows a single control panel to be active at a given time, to prevent instruction multiple contradictory instructions being issued simultaneously.

Risk: Medium

Pre-Conditions:

1. Require 2 (or more) control panels set up properly, and referred to as Control Panel A and B.
2. User must have valid credentials.

Steps:

1. Attempt to Login into Control Panel A

Test Case	Test Inputs	Expected Result	Post condition
Control Panel B is inactive	None	Login Successful	Move to Main Menu
Control Panel B is active	None	Login Failed	Display Popup that Another Control Panel is active.

2.1.8. Change Password

The system allows the user to change the password, but only if provided with the previous password first.

Risk: Low

Pre-conditions:

1. User must be logged in
2. User must have a current password
3. The password strength check module must be active (to check strength of new password).

Steps:

1. Go to Change Password Section.
2. Enter Current Password (Field 1)
3. Enter New Password (Field 2)
4. Re-enter New Password (Field 3)

5. Press the *Change Password* Button

Test Case	Test Inputs	Expected Result	Post condition
Enter Valid Current Password, Valid New Password, and Fields 2 and 3 are equal	Fields 1, 2, 3	Password Change succesful	User redirected to Main Menu
Enter Valid Current Password, Valid New Password, but Fields 2 and 3 are unequal	Fields 1, 2, 3	Password Change failed	Show Popup that Fields 2 and 3 do not match.
Enter Valid Current Password, Invalid New Password, and Fields 2 and 3 are equal	Fields 1, 2, 3	Password Change failed	Show Popup that New password is not strong enough.
Enter Invalid Current Password, Valid New Password, and Fields 2 and 3 are equal	Fields 1, 2, 3	Password Change failed	Show Popup that Current password incorrect.

2.2. User Interface Functionality Testing

2.2.1. Sensor Toggle

The Sensors Option allows the user to disable or enable specific sensors, as well as toggle the surveillance cameras. This is important to allow the user to choose its balance between privacy and security.

Risk: High

Pre-Condition:

1. User is logged in.

Steps:

1. Go to Sensors Option in the Menu Bar
2. Select some configuration of sensors and cameras.
3. Go to View Layout.
4. Check that the actual configuration matches the user configuration.

Test Case	Test Inputs	Expected Result	Post condition
Activate all Sensors and Cameras	User Configuration	Actual Configuration matches user configuration.	All sensors and cameras are active and working.
Activate all Sensors, Deactivate Cameras	User Configuration	Actual Configuration matches user configuration.	All sensors are active and working. All cameras are disabled.
Activate all Cameras, Deactivate all sensors	User Configuration	Actual Configuration matches user configuration.	All cameras are active and working. All sensors are disabled.
Deactivate all Sensors and Cameras	User Configuration	Actual Configuration matches user configuration.	All sensors and cameras are disabled.
Deactivate all Motion Sensors, Activate rest	User Configuration	Actual Configuration matches user configuration.	Only Motion Sensors are disabled.
Deactivate all Proximity Sensors, Activate rest	User Configuration	Actual Configuration matches user configuration.	Only Proximity Sensors are disabled.
Deactivate all Smoke Sensors, Activate rest	User Configuration	Actual Configuration matches user configuration.	Only Smoke Sensors are disabled.
Deactivate all Motion and Proximity Sensors.	User Configuration	Actual Configuration matches user configuration.	Only Motion and Proximity Sensors are disabled.

2.2.2. System Mode

The system can be in 2 different modes: user indoor / user outdoor. Indoor mode should disable all motion sensors inside the house as inactive, whereas Outdoor enables all sensors. Assuming that system mode is decided based on location of user's mobile device with respect to the house, unless overridden by user.

Risk: Medium

Pre-Condition:

1. User must be logged in
2. System must have location access for both home and mobile device.

3. In case of no set mode, mode set to indoor if distance between house and mobile device less than threshold (default 100m)

Test Case	Test Inputs	Expected Result	Post condition
User sets Indoor Mode	mobile device Location, Home Location	System set to Indoor Mode	All sensors and cameras within the home deactivated
User sets Outdoor Mode	mobile device Location, Home Location	System set to Outdoor Mode	All sensors and cameras activated
User does not set mode; mobile device close to Home	mobile device Location, Home Location	System set to Indoor Mode	All sensors and cameras within the home deactivated
User does not set mode; mobile device far away from Home	mobile device Location, Home Location	System set to Outdoor Mode	All sensors and cameras activated

2.2.3. Check Recorded Videos

The user can watch recorded footage of the surveillance zone for upto 7 days prior. Footage older than 7 days is moved into secondary storage, and not directly accessible by the user.

Risk: Medium

Pre-Condition:

1. Camera should have been running for 7 days (or more)
2. User must be logged in

Steps:

1. Go to View Surveillance Footage
2. Search for footage at any given time, upto 7 days previously.

Test Case	Test Inputs	Expected Result	Post condition
User searches for 1-day old footage	Search Date = 1 day before	Some footage found	Return all video segments found for given search condition
User searches for 4-day old footage	Search Date = 4 day before	Some footage found	Return all video segments found for given search condition
User searches for 7-day old footage	Search Date = 7 day before	Some footage found	Return all video segments found for given search condition
User searches for 10-day old footage	Search Date = 10 day before	No footage found	Return Error message "Date more than 7 days ago, videos shifted to Secondary Storage"

2.3. Communication Module

This stage of testing will check if the system can send correct notifications to the user and company, given that the sensor outputs are artificially generated and send to the communication modules.

2.3.1. User Notification via mobile device Call / Message

In case of anomaly, send a notification to the user's mobile device.

Risk: Medium

Pre-Conditions:

1. User has a valid account
2. User has specified a mobile device-number.

Steps:

1. Simulate activating certain sensor.
2. Pass sensor output to communication module.
3. Check View / View Layout in Menu, for Post-condition

Test Scenario	Test Inputs	Expected Result	Post condition
Activate Motion Sensor	Motion Sensor Outputs	User Notification, that door has been opened.	View Layout should show that specific door has been opened.

Test Scenario	Test Inputs	Expected Result	Post condition
Activate Smoke/Flame Sensor	Smoke/Flame Sensor Outputs	User Notification, that there is a fire.	View should display the surveillance zone, where there might be a fire.
Activate Proximity Sensor	Proximity Sensor Outputs	User Notification, that there is human movement outside.	View should display video feed outside the home.
No Sensors Activated	None	No notifications sent.	No change in state of system

2.3.2. Send Logs to Security Company

The system can send logs to the security company, in case of any alarm. It is necessary this step is always performed, so that the security company can respond in case of urgent alarms, as well store information which might be of use to the user.

Risk: Low

Pre-Conditions:

1. User has a valid account

Steps:

1. Simulate activate certain sensor.
2. Pass sensor output to communication module.
3. Check whether New Logs submitted to the Company, as User Log Files.

Test Scenario	Test Inputs	Expected Result	Post condition
Activate Motion Sensor	Motion Sensor Outputs	New Logs submitted to Company, regarding activation of motion sensors	View Layout should show that specific door has been opened.
Activate Smoke/Flame Sensor	Smoke/Flame Sensor Outputs	New Logs submitted to Company, regarding activation of smoke/flame sensors	View should display the surveillance zone.
Activate Proximity Sensor	Proximity Sensor Outputs	New Logs submitted to Company, regarding activation of proximity sensors	View should display video feed outside the home.
No Sensors Activated	None	No New Logs submitted to Company	No change

2.3.3. Panic Mode

The Emergency button can be used to trigger *panic mode*, in which the system can call a pre-defined number for the ambulance services.

Risk: High

Pre-Conditions:

1. User has a valid account

Steps:

1. Simulate activation of Panic Mode.
2. Check whether Ambulance services are contacted.

Test Scenario	Test Inputs	Expected Result	Post condition
Panic Mode Activated	None	Ambulance Services are contacted	No change
Panic Mode Not Activated	None	Ambulance Services are not contacted	No change

2.3.4. Alert Law Enforcement / Fire Management

The Communication Module should be able to alert the required enforcement teams, in case of serious anomalies, such as intrusion, fire alert, etc.

Risk: High

Pre-Conditions:

1. User has a valid account

Steps:

1. Simulate activate certain sensor.
2. Pass sensor output to communication module.
3. Check whether correct authorities are alerted to the situation

Test Scenario	Test Inputs	Expected Result	Post condition
Activate Motion Sensor	Motion Sensor Outputs	Law Enforcement Contacted, for Possible Intrusion / Theft	View Layout should show that specific door has been opened.
Activate Smoke/Flame Sensor	Smoke/Flame Sensor Outputs	Fire Management Contacted, for possible Fire	View should display the surveillance zone.
No Sensors Activated	None	No Authority Contacted.	No change

3. System and Integration Testing

This stage of testing assumes that all unit tests have concluded, and the different parts have been assembled together. The system's response to multiple situations is to be tested.

3.1. Response to Anomalous Activity

The ability of the system to respond to anomalous activities, such as theft, intrusion, or any emergency, is incredibly important, and requires multiple different units to perform with near-perfect precision. Hence it is necessary to perform Rigorous System Testing for these situations.

3.1.1. No Anomalous Activity

Pre-Condition: None

Expected Result: No action taken by system. No change in state.

Post-Condition: None

3.1.2. Door has been Opened

Pre-Condition:

1. Monitoring Doors Option Enabled. (I.e. User Outdoor Mode)
2. Motion Sensors Active

Expected Result: Notification sent, that door has been opened.

Post-Condition: 1. View Layout shows which door has been opened 2. Send Log to Security company 3. Display Reason of Caution on Control Panel.

3.1.3. Fire / Smoke Detected

Pre-Condition: Smoke Detection Sensors / Flame Sensors Active.

Expected Result:

1. Send Notification that there is a fire detected.
2. Send Alert to Fire Department after specified Time Delay

Post-Condition: 1. Send Log to Security company 2. Display Reason of Caution on Control Panel.

3.1.4. Outside Movement Detected.

Pre-Condition: Proximity Sensors must be active.

Expected Result: Send Notification that outside movement detected.

Post Condition: 1. Send Log to Security company 2. Display Reason of Caution on Control Panel.

3.1.5. Intrusion Detected

Pre-Condition:

1. Proximity and Motion Sensors must be active
2. System must be in User Outdoor Mode

Expected Results:

1. Send Notification of detected intrusion.
2. Notify Law Enforcement after specified Time Delay.
3. Activate Siren.

Post-Condition:

1. Send Log to Security company
2. Display Reason of Caution on Control Panel.

3.1.6. Emergency Button Pressed

Pre-Condition: None. Emergency Button always enabled.

Expected Results: Notify Nearest Hospital Services.

Post-Condition:

1. Send Log to Security company
2. Display Reason of Caution on Control Panel.

4. Constraints

The system must also pass the given performance, and storage constraints, as detailed by the SRS

4.1. Performance Constraints

- Ideally, considering a fully-functional internet connection, working sensors, and no power cuts, the system should be able to work 24 hours a day, seven days a week.
- The video feed displayed on the LCD should be as close to real-time as possible.
- The latency between detecting an anomaly and informing the customer should be as low as possible, typically *less than 5 seconds*.
- Whenever the user switches any mode or toggles any sensor, the system should perform the required action *within a few seconds*.

4.2. Storage Constraints

- The system should store video footage worth a week in the primary storage region. This means approximately around 170 hours of footage, per camera
- Secondary storage should always be free to move out the old records whenever the user intends to. The system should also backup the camera records every week to the secondary storage.