|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| REV | Change history | Zone | Changed By  Date | Approved  Date |
| 01 | Initial Draft | ALL | Shalini  04/02/20 | 04/06/20 |
|  |  |  |  |  |
|  |  |  |  |  |

1. **Introduction**

This document contains the Preliminary Hazard Analysis (PHA) for Real Estate Desktop Application.

1. **Purpose**

Preliminary hazard analysis (PHA) is a semi-quantitative analysis that is performed to:

**a.** Identify all potential hazards and accidental events that may lead to an accident

**b.** Rank the identiﬁed accidental events according to their severity

**c.** Identify required hazard controls and follow-up actions.

1. **Weak Authentication and Session Management** This is when attacks take advantage of improper authentication or session management practices and can lead to revealing sensitive information like passwords.

|  |  |  |
| --- | --- | --- |
| Risk ID | Risk | Rank |
| R-001 | Weak Authentication and Session Management | 5 |
| R-002 | Insecure Direct Object References | 3 |
| R-003 | Using Components with Known Vulnerabilities | 4 |
| R-004 | Injection | 1 |
| R-005 | Security Misconfiguration | 2 |

## Insecure Direct Object References Insecure direct object references lead to unauthorized data access. The most common that most people have heard of is called Local File Inclusion. This is where a secure file shows up on the front end of a Application

## Using Components with Known Vulnerabilities This is pretty self-explanatory and probably the easiest thing to avoid. Hackers can bypass old security measures easily. Simply, keep track of the software versions your application is using and monitor the security of the components through public notifications like mailing lists. Lastly, remember to follow the policies which software components are acceptable.

1. **Injection:** There’s a lot of different kinds of injections, targeted at different kinds of subsystems. The essential thing they let you do is they let you bypass protections and do unintended things and access data you weren’t intended to access.

## Security Misconfiguration If your security configuration is outdated, or not set up properly this can lead to unintended access to data or application functions.

|  |  |  |
| --- | --- | --- |
| Risk ID | Hazard | Hazard Control |
| R-001 | Weak Authentication and Session Management | user management and authentication is important. You should perform user and role validation on all actions |
| R-002 | Insecure Direct Object References | You can ensure access control checks when using direct object references and use reference maps instead of direct references. |
| R-003 | Using Components with Known Vulnerabilities | keep track of the software versions your application is using and monitor the security of the components through public notifications like mailing lists. |
| R-004 | Injection | enforce input type and length, ensure special characters are escaped, validate all input fields and use and input validation whitelist, and avoid dynamic queries or commands. |
| R-005 | Security Misconfiguration | repeatable and testable hardening process and regular updating and patching processes. If you’re diligent about security, you are way less likely to be hacked |
|  |  |  |

**3.Definitions N/A**

|  |  |
| --- | --- |
| **Probability** | **Criteria** |
| 1. Virtually Non-existent | Injection |
| 2. Remote | When the security is outdated |
| 3. Low | If the software versions are not updated |
| 4. High | Database failure |
| 5. Extremely High | If there is a case of improper authentication, then the probability would be extremely high |

|  |  |
| --- | --- |
| **Severity** | **Criteria** |
| 1. Almost None | The user will be unaffected, since the application is a desktop application. |
| 2. Slight | The user stays unaffected since we keep out security platforms updated. |
| 3. Marginal | The software versions are outdated the users are at the point of getting hacked easily. Users are very dissatisfied. |
| 4. Critical | Potential for serious problem for the user.Users might be dissatisfied as they might get hacked because of using local file system.  Or in case of a database failure. |
| 5. Extremely Critical | Application is not functional as anybody can hack into the desktop application |

**PHA Severity Chart**

**4. PHA Risk Chart 5 x 5 Matrix :**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  | Probability | | | | | |
|  | |  | 1 Virtually Non-existent | 2   Remote | | 3   Low | 4   High | 5  Extremely High |
| Severity | | 1 Almost none | 1 | 2 | | 3 | 4 | 5 |
| 2 Slight | 2 | 4 | | 6 | 8 | 10 |
| 3 Marginal | 3 | 6 | | 9 | 12 | 15 |
| 4 Critical | 4 | 8 | | 12 | 16 | 20 |
| 5 Extremely critical | 5 | 10 | | 15 | 20 | 25 |
|  | = Risk Acceptable | | | |
|  | = Risk Unacceptable without further investigation | | | |
|  | = Risk Unacceptable without controls | | | |
|  |  | | | |

1. **Risk Categories**

The following risk categories shall be considered as potential hazards for the Real Estate Desktop Application

1. Software
2. Hardware
3. Usability
4. Manufacturing
5. Implementation
6. Environment
7. Labeling

**6.References**

[**https://wpengine.com/blog/10-critical-application-security-risks/**](https://wpengine.com/blog/10-critical-application-security-risks/)

[**https://www.researchgate.net/figure/A-consequence-table-should-be-prepared-in-advance-of-the-PHA\_tbl1\_237454644**](https://www.researchgate.net/figure/A-consequence-table-should-be-prepared-in-advance-of-the-PHA_tbl1_237454644)

[**https://software.intel.com/security-software-guidance/insights/how-assess-risk-your-application**](https://software.intel.com/security-software-guidance/insights/how-assess-risk-your-application)

[**https://www.researchgate.net/figure/PHA-intensity-levels\_tbl1\_223621770**](https://www.researchgate.net/figure/PHA-intensity-levels_tbl1_223621770)

[**https://www.pharmaceuticalonline.com/doc/using-preliminary-hazard-analysis-to-determine-equipment-and-instrument-requalification-frequency-0001**](https://www.pharmaceuticalonline.com/doc/using-preliminary-hazard-analysis-to-determine-equipment-and-instrument-requalification-frequency-0001)

| **1. HAZARD: Software** | | | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Risk ID | Foreseeable Sequence of events | Hazardous Situation | Potential Harm | Risk Estimation (Currently Pre-Recommendation) | | | Risk Control Measures (Currently Risk Controls) | | | | Residual Risk (Currently Post-Recommendation) | | | Risk/ Benefit Analysis | Notes |
| Severity | Probability | Risk Value & Acceptability | Inherent Safe Design | Protective Measures | Information for Safety | Verification of Implementation | Severity | Probability | Residual Risk Value & Acceptability |
| 1.1 | 1. Database failure. | 1. Known loss of system functionality | 1. Facility must revert to Pre-system practices. | Minor | Occasional | R1 – Acceptable Risk: Negligible | (List current risk control specifications)  SPC-006 | (List addition protective measures specification(s)) | (List any cautions, warnings, information messages to be added to the User or Service Manual) | (List Test Case(s))  TST-006 | Minor | Occasional | R1 – Acceptable Risk: Negligible | None required |  |

| **2. HAZARD: Hardware** | | | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Risk ID | Foreseeable Sequence of events | Hazardous Situation | Potential Harm | Risk Estimation (Currently Pre-Recommendation) | | | Risk Control Measures (Currently Risk Controls) | | | | Residual Risk (Currently Post-Recommendation) | | | Risk/ Benefit Analysis | Notes |
| Severity | Probability | Risk Value & Acceptability | Inherent Safe Design | Protective Measures | Information for Safety | Verification of Implementation | Severity | Probability | Residual Risk Value & Acceptability |
| 2.1 | 1. Hardware component fails  2. Loss of ability to communicate with network | 1. Known loss system functionality | 1. Facility must revert to Pre-system practices | Minor | Occasional | R1 – Acceptable Risk: Negligible | SPC-OO4 | NONE | USER UNABLE TO OPEN THE APPLICATION AND IT SAYS SOMETHING WENT WRONG FROM OUR SIDE | TST-004 | Minor | Occasional | R1 – Acceptable Risk: Negligible | None required |  |

| 3. **HAZARD: Usability (Main Usage)** | | | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Risk ID | Foreseeable Sequence of events | Hazardous Situation | Potential Harm | Risk Estimation (Currently Pre-Recommendation) | | | Risk Control Measures (Currently Risk Controls) | | | | Residual Risk (Currently Post-Recommendation) | | | Risk/ Benefit Analysis | Notes |
| Severity | Probability | Risk Value & Acceptability | Inherent Safe Design | Protective Measures | Information for Safety | Verification of Implementation | Severity | Probability | Residual Risk Value & Acceptability |
| 3.1 | 1. User giver wrong information during Register or Login. | 1. System functionality loss | 1.User unable to use the application  2.user gets frustrated | Minor | Remote | R1 – Acceptable Risk: Negligible | SPC-001 TO SPC-003 | NONE | USER WILL SEE A POPUP ABOUT WHAT MISTAKE HE/SHE IS DOING | TST-001 AND TST-002 | Minor | Remote | R1 – Acceptable Risk: Negligible | USER MUST ABLE TO CORRECT THE MISTAKE AND ABLE TO LOGIN OR REGISTER |  |

| **4. HAZARD: Manufacturing** | | | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Risk ID | Foreseeable Sequence of events | Hazardous Situation | Potential Harm | Risk Estimation (Currently Pre-Recommendation) | | | Risk Control Measures (Currently Risk Controls) | | | | Residual Risk (Currently Post-Recommendation) | | | Risk/ Benefit Analysis | Notes |
| Severity | Probability | Risk Value & Acceptability | Inherent Safe Design | Protective Measures | Information for Safety | Verification of Implementation | Severity | Probability | Residual Risk Value & Acceptability |
| 9.1 | 1.Application does not work.  2.Admin unable to enter information regarding the properties | 1.fault production of the application | 1.user unable login to the application.  2.user unable to see the information regarding the properties | Minor | Improbable | R1 – Acceptable Risk: Negligible | SPC-OO9 AMD SPC-010 | 1Admin must be notified. | 1.User must be notified Regarding the Technical Issues | TST-008 AND TST-009 | Minor | Improbable | R1 – Acceptable Risk: Negligible | None Required |  |

| **5. HAZARD: Implementation/Environment** | | | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Risk ID | Foreseeable Sequence of events | Hazardous Situation | Potential Harm | Risk Estimation (Currently Pre-Recommendation) | | | Risk Control Measures (Currently Risk Controls) | | | | Residual Risk (Currently Post-Recommendation) | | | Risk/ Benefit Analysis | Notes |
| Severity | Probability | Risk Value & Acceptability | Inherent Safe Design | Protective Measures | Information for Safety | Verification of Implementation | Severity | Probability | Residual Risk Value & Acceptability |
| 5.1 | 1.Application installed in unsupported devices or in the wrong platform .  2. System does not operate as intended. | 1. Application functionality impaired | 1. User unable to use the application features | Serious | Remote | R2: Acceptable with risk minimization | SPC-011 AND SPC-012 | 1. User must follow the installation protocols. | 1. user must notified that this application does not support the specific platform.  2. user must see the installation protocols before the installation | TST-010 AND TST-013 | Serious | Remote | R2: Acceptable with risk minimization | Checkout procedures are completed once installation is complete. This prevents inoperable system to be implemented. |  |

| **6. HAZARD: Labeling** | | | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Risk ID | Foreseeable Sequence of events | Hazardous Situation | Potential Harm | Risk Estimation (Currently Pre-Recommendation) | | | Risk Control Measures (Currently Risk Controls) | | | | Residual Risk (Currently Post-Recommendation) | | | Risk/ Benefit Analysis | Notes |
| Severity | Probability | Risk Value & Acceptability | Inherent Safe Design | Protective Measures | Information for Safety | Verification of Implementation | Severity | Probability | Residual Risk Value & Acceptability |
| 7.1 | 1. Information for use not provided to user.  2. User does not know how to use the device. | 1. User cannot use the system | 1.User gets frustrated and uninstall the application. | Minor | Improbable | R1 – Acceptable Risk: Negligible | Spec-013 | 1.Application developer must create the perfect set of guidelines. | 1. user must be provided with the clear set of guidelines regarding the installation | Tst-012 | Minor | Improbable | R1 – Acceptable Risk: Negligible | None Required |  |
| 7.2 | 1. Information for use provided to user is unclear.  2. User does not know how to use the device. | 1. User cannot use the system | 1.User gets navigated to the unknown pages by pressing the wrong buttons.  2. User will see the unexpected results | Major | Improbable | R1 – Acceptable Risk: Negligible | Spec-014 | 1.Application Developer must label the every field appropriately. | 1. Every button must be labelled perfectly so the user can navigate easily. | Tst-013 | Minor | Improbable | R1 – Acceptable Risk: Negligible | None Required |  |