|  |  |  |  |
| --- | --- | --- | --- |
| HyperIT Tech Bhd | QUALITY ASSURANCE PLAN | REVISION | 01 |
| PAGE | 1 of 24 |
| QUALITY ASSURANCE PLAN  Prepared By: Checked By: Approved By:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Izzati Husna Athirah Fauzi Pn Mawarwiduri System Analyst Project Manager/Functional Manager Director | | | |
| HyperIT Tech Bhd | QUALITY ASSURANCE PLAN | REVISION | 01 |
| PAGE | 2 of 24 |
| **TABLE OF CONTENTS**  **7.1 OBJECTIVE………………………………………………………………………………………………………………??**  **7.2 QUALITY POLICY……………………………………………………………………………………………………..??**  **7.3 PRELIMINARY PLAN:**   * + 1. **EXCEPTION HANDLING………………………………………………………………………………??** * **Risk Analysis…………………………………………………………………………………??**   + 1. **PROCEDURES………………………………………………………………………………………….…??**   **Change Request Procedure………………………………………………………………………..??**  **7.4 EVENT IDENTIFICATION……..……………………………………………………………………………………??**  **7.5 STANDARDS FOR DOCUMENTATION TESTING………………………………………………………………………………………………………………….??**  **7.6 SERVICE LEVEL AGREEMENTS……………………………………………………………………………………??** | | | |
| Company’s Logo | QUALITY ASSURANCE PLAN | REVISION | 01 |
| PAGE | 1. of 24 |
| * 1. **OBJECTIVES**   The objective of the HyperIT Tech Bhd in producing this Quality Assurance Plan is as following:   * 1. To ensure that the software being produced is in good quality and able to achieve the customer’s expectation.   **7.2 QUALITY POLICY**  The quality policies for the HyperIT Tech Bhd are as following: -   * 1. To provide clients with the highest attainable quality in their services. All the company’s services will be acceptable for their standard use and delivered in conformance with the client’s quality specifications.   2. To work towards the comprehensive client satisfaction and total services reliability including software maintenance. In order to accomplish this, HyperIT Tech Bhd operates under a quality management system that is reviewed at planned intervals to ensure its continuing suitability and effectiveness. This continuous review assures their clients that the services they provide meet or exceeds their expectations.   **7.3PRELIMINARY PLAN**  The preliminary plan is divided into 5 main area as following   * + 1. Exception Handling     2. Procedure – Change Control Procedure     3. Event Identification     4. Standard Documentation and Testing     5. Service Level Agreement     6. **Exception Handling**   Error handling refers to programming, application and communication errors being anticipated, detected, and resolved. It is method that can is used to solve the problem occurs   * Risk Analysis   In determining risks associated with the e-Donation Application, we utilized the following model for classifying risk:  Risk = Threat Likelihood x Magnitude of Impact  And the following definitions:  Threat Likelihood   |  |  | | --- | --- | | **Likelihood (Weight Factor)** | **Definition** | | High (1.0) | The source of the threat is highly motivated and sufficiently capable, and controls are ineffective to prevent the vulnerability | | Medium (0.5) | The threat source is motivated and capable, but there are controls in place that can impede the vulnerability's successful exercise. | | Low (0.1) | The threat source lacks motivation or ability, or controls are in place to prevent the vulnerability from being exercised, or at least significantly impede it |   Magnitude of Impact   |  |  | | --- | --- | | Component | Description | | High (100) | The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.  Examples:   1. Major data loss includes all the data of donation application, the applicant’s details and yearly report of donation 2. Major financial loss such as the amount of the donation | | Medium (50) | The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.   1. Significant data loss includes all the data of donation application, the applicant’s details and yearly report of donation 2. Significant financial loss such as the amount of the donation. | | Low (10) | The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.   1. Minor data loss includes all the data of donation application, the applicant’s details and yearly report of donation 2. Minor financial loss such as the amount of the donation |   Risk was calculated as follows:   |  |  |  |  | | --- | --- | --- | --- | | Threat Likelihood | Impact | | | | Low (10) | Medium (50) | High (100) | | High (1.0) | Low Risk (10 x 1.0 = 10) | Medium Risk (50 x 1.0 = 50) | High Risk (100 x 1.0 = 100) | | Medium (0.5) | Low Risk (10 x 0.5 = 5) | Medium Risk (50 x 0.5 = 25) | Medium Risk (100 x 0.5 = 50) | | Low (0.1) | Low Risk (10 x 0.1 = 1) | Low Risk (50 x 0.1 = 5) | Low Risk (100 x 0.1 = 10) |   Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)  The following potential vulnerabilities were identified.   |  |  | | --- | --- | | **Vulnerability** | **Description** | | Password strength | Passwords used by the web application is not strong which do not require special characters and numbers. Attackers could guess the password of a user to gain access to the system. | | Disaster recovery | There are no procedures for ensuring the system's continued operation in the case of a major company disruption or catastrophe. | | Lack of Documentation | The progress of the system from the planning stage to the implementation is not documented for future reference. |  Threat Statement The team identified the following potential threat-sources and associated threat actions applicable to the e-Donation Application.   |  |  | | --- | --- | | **Threat-Source** | **Threat Actions** | | Hacker | * Unauthorized system access. * Steal user’s information (personal information) | | Computer Virus | * Worms (Spread from computer to computer, but unlike a virus it has the capability to travel without any human action) * Trojan Horse | | Computer Criminal | * Spoofing (Is a sort of scam where criminals try to acquire private data from someone) * Identity Theft (is when thieves steal your personal information in order to take over or open new accounts) | | Environment | * Natural disaster |  |  |  |  |  |  | | --- | --- | --- | --- | --- | | Threat/Likelihood | Magnitude of Impact | | | | | High (1.0) | 10 | 50 | 100 | | Hacker |  |  | Risk:  100 x 1.0 =100 | | Medium (0.5) |  | | | | Computer Virus |  | Risk:  50 x 0.5 = 25 |  | | Computer Criminal |  |  | Risk:  100 x 0.1 =100 | | Low (0.1) |  | | | | Environment |  |  | Risk:  100 x 1.0 =100 |      * + 1. **Procedure** * Change Request Procedure   A change request is a significant document that is component of the change management process as it sets out the information and reasons for the change in an application or system. (Techopedia.com, n.d.)  Change Control Procedure is the process used by a company to document, recognize and authorize modifications in an IT environment. It decreases the likelihood of unauthorized modifications, disruptions and mistake.  Change Request Procedures is representing steps of 6 as below.   1. Identification of potential changes   Changes request will be identified by project manager from any stakeholders. Client requests to add a new requirement that generates a report based on type of organization or department rather than an annual report. The project manager will recognize these modifications and discuss them further   1. Analysis of change request   Project manager evaluate the potential change by doing feasibility study to ensure the worthiness of the potential change. Project manager will discuss the changes with the team members. To assess the suitability for the project, the changes will be evaluated. The feasibility study will be carried out to ensure that the changes are worthwhile.   1. Evaluation of change request   The project manager will also address the effect of implementing the change with team member, client, in order to comply with the possible modifications. If all the stakeholders agree on the discussion, the next step will be followed by the modifications. If no agreement has been reached, it will not proceed with the modifications.   1. Planning of change   If the request for change has been agreed, the potential changes will be prepared for a project plan. If the request for modification has not been agreed, no planning will take place   1. Implementation   The change request will be implemented in accordance with the plan. Monitoring of the implemented changes will be done. Monitoring is performed through evaluation, testing, and verification. So that the changes implemented can be successful   1. Reviewing and closing   Project Manager will conduct checks and reviews to confirm the improvements made. The change control cycle is complete if the modifications have been effectively completed. Review and close will not be performed if stakeholders have not agreed on the request for change. | | | |
| Company’s Logo | QUALITY ASSURANCE PLAN | REVISION | 01 |
| PAGE | 1. of 24 |
| * + 1. EVENT IDENTIFICATION   Events Identification is the method of defining critical occurrences in the life cycle of software development to confirm that system development is on the correct track of the final project being created.   1. Walkthrough   Walkthrough is step by step test to verify if all aspects of an environment, plan or process is ready for its intended purpose.   1. Review   Review is referred to the process of examination for defects by individuals other than the person who produced it   1. Inspection   Inspection is an engineering practice to detect and correct software artifact flaws and to prevent them from leaking into field activities.  Quality Assurance Tools which are walkthrough, review and inspection will be used in every phase of system development as below.   1. System Planning    * + - Review Project Plan        - Walkthrough the project scope and objectives        - Review feasibility analysis report.        - Inspects of Quality Assurance Plan 2. System Analysis  * Walkthrough data gathering. * Review and inspect System Requirement Specification  1. System Design  * Walkthrough database design. * Walkthrough system process * Walkthrough interface system * Review and inspect System Design Specification  1. Implementation  * Review test plan * Inspect codes   + 1. STANDARDS FOR DOCUMENTATION AND TESTING * The standards that is being used in producing quality documentation is Harvard Referencing /IEE * the methods of testing that is being used in validating user’s requirements is Black box, UAT, Quality Control (Walkthrough, Inspection, Review)   + 1. SERVICE LEVEL AGREEMENTS   Explain what is service level agreement:  A **service-level agreement** (**SLA)** is a contract between a service provider and its inner or external clients to document the services that the supplier will provide and define the service requirements that the supplier is required to fulfill.   * Introduction – The purpose of this SLA is a document of mutual agreement between HyperIT Tech Bhd and KPM Beranang in developing e-Donation Application. * Scope of work – The agreement involved development’s time duration which is 3 Months and the development cost which is RM15, 300, under agreed scope which is hardware cost, software cost, development cost, utilities bill, staff salary and system maintenance by HyperIT Tech Bhd to deliver complete products   + Services Providences * Warranty – The warranty is to provide correction to the system in 6 months after delivery of the system. After 6 months, cost is under client’s responsibility.   + - Service Period and Time – The duration for system maintenance of e-Donation application is 1 time per month for 2 year)     - Hardware & Software – Agreed hardware and software specification  |  |  | | --- | --- | | Specification | Adobe Dreamweaver CS6 | | Processor | Intel® Pentium® 4 or AMD Athlon® 64 processor | | Memory | 512 MB of RAM | | Hard disk | 1 GB of available hard-disk space for installation; additional free space required during installation | | Graphic Display | 1280 x 800 display with 16-bit graphics adapter |  * + - Optional Request – For other request, it will follow the service period and time and also in term of warranty that has been agreed. If additional request are made after the warranty period, the charges will be made accordingly to the degree of request made.     - Compensation – HyperIT tech Bhd will make compensation if the error or failure of the system is because of developer’s team fault. | | | |