Quality Plan

*Hybrid Cryptography for Automated Election System*

1. **Introduction**

The quality plan for the Hybrid Cryptography for Automated Election System defines the responsibilities and procedures to be adopted to ensure that the data and information produced as part of Project 131 are reliable, fit for purpose, consistent with documented objectives and deliverables. It summarises the system of internal management that governs the decisions and instructions concerning project quality assurance. Moreover, the purpose of developing a quality plan is to produce the customer’s expectations in terms of quality and prepare a proactive quality management plan to meet those expectations.

**2. Project Contractual Information**

|  |  |
| --- | --- |
| Project: | Hybrid Cryptography for Automated Election System |
| Project Number: | 131 |
| Programme Co-ordinator: | Mr. Sebastian Sanchez |
| Principal Investigators(s): | **NA** |

**3. Scope of Work and Quality Objectives**

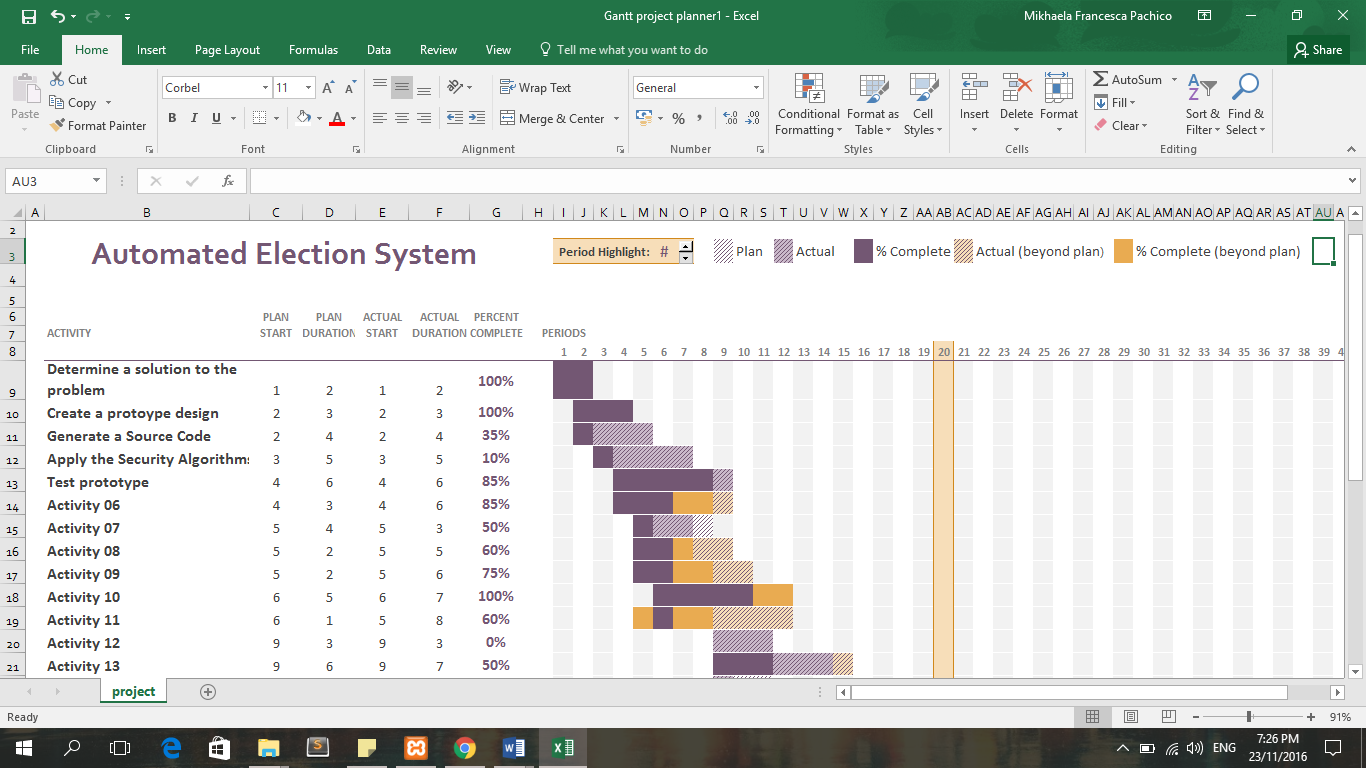
|  |  |
| --- | --- |
| Scope of work: | The scope of the study would only include the issues and possible solutions for the security of the transmission of election returns on the server-level of the automated election system in the Philippines. Further study on the other parts of the automated election system will no longer be covered. |
| QA Requirement: | Must be able to address the problem specifically on the server level of the Philippine Automated Election System. The proposed system must be able to comply with the standards. |

**4. Project Organisation**

|  |  |
| --- | --- |
| Project Manager(s): | Joanna Hipolito, Project Manager |
| Task Manager(s): | Mikhaela Pachico, Project Developer  Monique Jovellano, Project Developer |
| Quality Assurance: | Joanna Hipolito, Quality Assurance Manager |
|  |  |
| Other Team Members: | Mikhaela Pachico, Performance Analyst  Monique Jovellano, Test Analyst |
| Subcontractors: | NA |
| User Community: | Commission on Elections |
| Technical Reviews: | Mikhaela Pachico, Performance Analyst |

**5. Project Duration and Scheduling**

|  |  |
| --- | --- |
| Start Date: | September 19, 2016 |
| Completion Date: | December 12, 2016 |
| Scheduling of Activities: |  |



**6. Deliverables**

Deliverables specified for the project include:

1. An acceptable Quality Plan
2. An acceptable Data Management Plan (*Appendix YY*)
3. Progress Reports
4. Final Reports

**7. Review of Quality Plan**

The Quality Plan will be reviewed every week at consortium meetings. If there are changes to be made regarding the project or there are parts that needed modifications, then the members of the project team may call an emergency meeting. There will be member that is assigned to take notes of everything that has been discussed.

**8. Document and Record Control**

Project documents, records and data will be controlled and stored in the School of Computing and Information Technologies of Asia Pacific College. Field notebooks will be clearly labelled and made available for consultation by all members of the project team. All documents relating to the project will be stored in folders with clear and informative labels. Any additional folders will be shelved and labelled on their outer edge. All digital files will be stored on the computing network and frequently backed up, either centrally or by the individual member of staff. Staff assigned to keep the file should at least update the back-up files.

The Quality Plan and Data Management Plan will be issued to all members of the consortium.

Project Progress Reports will be issued to the following:

* Project Advisers
* Project Consultants

**9. Documented Procedures**

The proposed system was influenced by a research study on the security of an internet voting system. In that study, the researchers designed an Internet voting system applicable for worldwide voting which was based on Ohkubo et al.’s scheme combined with Public Key Infrastructure. In the system, voter’s privacy was guaranteed by using blind signature and mix-net, and robustness which was provided through the threshold encryption scheme. A way of typical implementation for internet voting system was proposed by employing Java technology. PKI allowed worldwide key distribution and “one certificate/one vote” policy. Therefore, anyone can participate as long as a certificate was given by Certificate Authority (CA). (Retrieved on August 27, 2016 / http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=311B92E00249A90FA1A9557F7E3ABA46?doi=10.1.1.6.1111&rep=rep1&type=pdf). In this study, it was showed it is possible to incorporate a PKI in a voting system. Not only it was possible, it was also recommended for security purposes of the sys-tem.

**10. Additional Information**

Unless included in associated technical procedures, any other information that has direct relevance to the quality of the product or service being provided should be included in the Quality Plan. This could include:

1. special requirements for the procurement of services or goods, including subcontractors;
2. additional procedures and controls for the review and verification of deliverables or other documents;
3. special requirements for the identification and traceability of products, including, where applicable, the traceability of staff performing specific duties;
4. special criteria for identifying the status of inspection and test products;
5. minimum qualifications, training or experience required of staff to undertake certain activities, or any specialist staff training;
6. process control requirements, including monitoring of activities;
7. special procedures for the handling, storage, packaging, preservation and delivery of product;
8. requirement for servicing of a product for which ongoing maintenance is required;
9. specialist statistical techniques required.

Prepared by: Date:

Monique Jovellano November 23, 2016

Project Developer

Checked by: Date:

Justin Pineda November 23, 2016

Project Adviser

Approved by: Date:

Manuel Sebastian Sanchez November 23, 2016

Professor