# Quality Management Plan – MAJTeQ

## Project Name: UltraSol Energy Solutions Merger

**Assigned Members:** Aidan Cadieux, Jamie Lewis, Matthew Telford, Quinn Parent, Taqi Zaidi
**Date Last Modified:** January 24, 2024
**Version:** 1.00

---

# Introduction

The approach to Quality Management for the UltraSol Energy Solutions IT infrastructure project is centered on ensuring the highest standards of efficiency, functionality, and security in all aspects of the project. Our methodology involves comprehensive testing, validation, and verification processes at every stage of the project lifecycle, from planning to execution and post-implementation review. We are committed to ensuring that every component of the IT infrastructure aligns with both industry best practices and the specific needs of UES.

# Quality Standards

Responsibility for Quality Certification: Quality assurance responsibilities are assigned to specialized teams within the MAJTEQ Consulting Group. This includes a dedicated IT Quality Assurance team for technology components and a Project Quality Manager for overall project quality certification.

- Quality Benchmarks for Project Elements:
  - Network Infrastructure: Quality standards include robustness, latency, throughput, and security compliance. Tests for network components include performance testing, security vulnerability assessments, and network load testing.
  - Cloud Systems and Data Governance: Adherence to data integrity, security standards (such as ISO/IEC 27001), and compliance with relevant data protection regulations. Quality checks include regular security audits and data integrity tests.
  - Server/Client Deployment: Focus on system reliability, scalability, and response times. Testing involves stress testing, scalability testing, and user acceptance testing.
- Testing Process for Major Elements:
  - Pre-Implementation Testing: Involves simulation environments to assess the performance of network setups, server configurations, and application deployments.

- Implementation Phase Testing: Conducted in a live environment, this includes real-time monitoring, load testing, and security testing.
- Post-Implementation Review: Includes user feedback analysis, system performance evaluation, and security audits.

# Problem Reporting and Corrective Action Process

## Issue Reporting Levels:

- Level 1 (Minor Issues): Handled internally within the respective technical teams. Includes minor software bugs or hardware compatibility issues.
- Level 2 (Moderate Issues): Requires reporting to the Project Quality Manager. These are issues that may impact project timelines or minor security concerns.
- Level 3 (Major Issues): Any major disruptions, security breaches, or significant delays must be escalated to the Project Steering Committee and UES senior management.

## Corrective Action Process:

- Immediate Assessment: Rapid evaluation of the issue to determine the impact and urgency.
- Containment Actions: Immediate actions to contain and limit the impact of the issue.
- Root Cause Analysis: Conducted to identify the underlying causes of the issue.
- Corrective Actions: Development and implementation of a plan to rectify the issue and prevent recurrence.
- Reporting and Documentation: Comprehensive documentation of the issue, the analysis, and the corrective actions taken.