**INSTRUCTIONS FOR RISK ACCEPTANCE FORM**

This form is to be used to acknowledged, justify, and/or document risk acceptance of a known deficiency. The responsible party that signs this document is ultimately acceptable all liability, risk, and responsibility associated with the decision represented in the document. It is highly recommended that a Compensating Control or Recommended Action be defined in order to mitigate risk and obtain full approval of risk acceptance.

**The items below must be completed:**

1. **NIST 800-53 Control Deficiency:**

Display the appropriate National Institute of Standards and Technology (NIST) control associated to the deficiency

1. **Description of the Deficiency:**

Provide a summary of the overall deficiency that was derived from <*Security or IT Team*> recommendation or third party assessment/audit.

1. **Justification for Risk Acceptance:**

Justify why a Risk Acceptance is requested or required versus remediating the deficiency.

1. **Description of the Compensating Control that will be put in place (if any):**

In order to obtain a Risk Acceptance or a deficiency, a compensating control must be put in place or justification of no compensating control should be explained.

A very detailed description must be provided, in writing, and the approving individuals on the form are accepting the compensating control. Attach additional documentation as needed.

1. **Additional Remarks:**

Provide any other comments and supporting material needed for the Risk Acceptance. If there is not sufficient room attach additional documentation as needed.

1. **Approvals**

Obtain necessary signatures (based on the various roles) in order for the Risk Acceptance to be submitted to the *<Company Name> Department of IT.*

1. **Risk Acceptance Expiration Date**

Cannot exceed one (1) year from the Responsible <*Party Name*> acceptance and approval date.

For additional questions, guidance, or details please contact the following:

*Department of IT – <Security/Governance Team>*

*<Security IT Group>@<domain>.com*

*<Phone or extension to Help Desk>*