|  |
| --- |
| Incident Response Plan  <IRP Template - System Name> |

# Purpose

*[A brief description of the purpose of this IRP, including why the IRP is required e.g. control requirement from security standard and guideline. Any regulations or procedures identified.]*

# Defination

*[Defination on what constitutes a cyber security incident, the types of incidents likely to be encountered and the expected response to each type e.g. incident impact matrix and response service level target.]*

# Role and Responsibility

*[List the roles and responsibilities involved in the incident response. Including the authority, or authorities, responsible for investigating and responding to cyber security incidents, and other parties which need to be informed in the event of a cyber security incident]*

# Incident Response Steps

*[Include the steps and stages to react to a security incident appropriately. Include the incident communication process, incident escalation process and any specific contingency measures]*

# Legal Procedure

*[Include the criteria by which an investigation of a cyber security incident would be requested from a law enforcement agency and the steps necessary to ensure the integrity of evidence relating to a cyber security incident]*

# Document Approvals

*[list of Approver/Endorsers of the document with Approval/Endorsement record]*

# Document Administration

## Document Location

*[Location where the document is stored]*

## Document References

*[List of documents referred to in the development of this document]*

## Amendment History

*[This document has the following amendment history]*

## Glossary

*[Glossary]*