# Document Control

## Versioning

|  |  |  |
| --- | --- | --- |
| **Name** | **Date** | **Reason** |
| Version 1 | February 1, 2019 | Placed into production |

## Applicable Parties

This document is strictly confidential and should only be distributed or viewed by the following parties:

* HAL Designated Associates
* HAL Regional Employees (Compartmented to the Division)
* HAL Management Team
* HAL Auditing Team

## Review Period

This document is subject to review by the Information Security Policy Committee (ISPC) at a minimum interval of quarterly (every 3 months) at a maximum interval of bi-annually (every 6 months).

### Previous Reviews

|  |  |  |
| --- | --- | --- |
| **Committee** | **Review Date** | **Approval Date** |
| ISPC | 7/15/2018 | 8/1/2018 |
| CEO | 1/21/2019 | 1/22/2019 |
| Corporate CIO | 1/23/2019 | 1/23/2019 |

# Purpose

The purpose of this policy is to provide guidelines for system management as implemented within the HAL network both within the network infrastructure, pertaining to workstations and server class computers.

# Scope

## Applicability

This policy applies to all HAL employees and affiliates at all HAL facilities and locations world-wide.

## Ownership

This policy is under the direct control of the HAL Corporate CIO with input from xx and other members of management with an interest in the program.

# Policy

## General Guidelines

## Basic Client Computer Configuration Policy

All computer systems must be configured according to the NIST checklist to ensure patHALng against the common system vulnerabilities. All systems must receive Operating System updates from the local Software Update Server, as dictated by the development team so as to ensure continued functionality of company proprietary software packages.

## Basic Server Computer Configuration Policy

All servers must be hardened against common system vulnerabilities using the NIST Guides and vendor security update announcements. The server infrastructure will receive updates via SUS to ensure thorough and consistent system configurations. There must be minimum level of security controls installed on each server to protect the infrastructure. All servers changes, updates, upgrades must be approved through the change proposal process and logged into a change management database with timestamps.

# Enforcement

Any employee found to be in violation this policy may be subject to disciplinary action, up to and including termination of employment.