# 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 CISO | 1/23/2019 | 1/23/2019 |

# Purpose

The purpose of this policy is to specify the requirement for utilizing anti-virus software and other control mechanisms to aid in the prevention of the introduction of malicious software ss to HAL corporate owned systems, where corporate owned is defined as any system operating in a HAL production environment on the company network, whether within the company owned facilities or issued to company agents or employees for use at remote locations for company business.

# 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 other members of management with an interest in the program.

# Policy

## General Guidelines

Always run the corporate standard, supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.

NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.

Delete spam, chain, and other junk email without forwarding, refer to HAL's *Acceptable Use Policy*.

Never download files from unknown or suspicious sources.

Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.

Always scan a floppy diskette from an unknown source for viruses before using it.

Back-up critical data and system configurations on a regular basis and store the data in a safe place.

If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, and then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

## Responsibility

Responsibility will befall to IS/IT/InfoSec staff to verify current anti-virus revisions and maintain the corporate download website with current updates for corporate assets.

# Enforcement

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