# 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 guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

# 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

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. HAL’s key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by InfoSec. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

# Enforcement

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

*NOTE: As part of the SECCDC event, infractions of the rules regarding this policy may result in a point penalty.*