# 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 provide guidance for the use of Intrusion Detection and Prevention Systems as implemented within the HAL network both within the network infrastructure and on the perimeter of the network.

# Scope

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

# Policy

## Guidelines

There must be a minimum of two network based Intrusion Detection and Prevention Systems running at all times on HAL’s network, both should be located at the perimeter of the network, at the firewall bordering the DMZ. The IDS signatures must be updated every 2 weeks from the vendor to keep the IDS(s) at current signature level. Any suspected intrusions, suspicious activity, or unexplained erratic system behavior discovered by administrators, users, or computer security personnel must be reported to the organizational IT computer security office within 1 hour and the Incident Response plan should be initiated. All intrusions with financial or customer data loss must be reported to CEO, CFO, CIO within 7 days of the loss.

Refer to the HAL Incident Response Plan for further details regarding events.

## Logging

The IDS logs must be kept for minimum of 1 year. The IDS Event logs must be monitored daily by InfoSec Staff for abnormal activities.

## Ownership

Responsibility for maintenance, including signature updates, firmware updates and system testing, as well as any future iterations of IDS implementations, will fall to the InfoSec team with ultimate approval from the CISO and InfoSec manager.

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.

# Enforcement

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