# 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 guidelines for Remote Access IPSec, or L2TP Virtual Private Network (VPN) connections to the HAL corporate network.

# Scope

## Applicability

This policy applies to all HAL employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the HAL network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

## 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

Approved HAL employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Policy*.

Additionally,

* It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to HAL internal networks.
* VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
* When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
* Dual (split) tunneling is NOT permitted; only one network connection is allowed.
* VPN gateways will be set up and managed by HAL network operational groups.
* All computers connected to HAL internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
* VPN users will be automatically disconnected from HAL's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
* The VPN concentrator is limited to an absolute connection time of 24 hours.
* Users of computers that are not HAL-owned equipment must configure the equipment to comply with HAL's VPN and Network policies.
* Only InfoSec-approved VPN clients may be used.
* By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of HAL's network, and as such are subject to the same rules and regulations that apply to HAL-owned equipment, i.e., their machines must be configured to comply with InfoSec's Security Policies.

# Enforcement

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