# 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 define standards for connecting to HAL's network from any host. These standards are designed to minimize the potential exposure to HAL from damages which may result from unauthorized use of HAL resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical HAL internal systems, etc.

# Scope

## Applicability

This policy applies to all HAL employees, contractors, vendors and agents with a HAL-owned or personally-owned computer or workstation used to connect to the HAL network. This policy applies to remote access connections used to do work on behalf of HAL, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

## 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

It is the responsibility of HAL employees, contractors, vendors and agents with remote access privileges to HAL's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to HAL.

General access to the Internet for recreational use by immediate household members through the HAL Network on personal computers is permitted for employees that have flat-rate services. The HAL employee is responsible to ensure the family member does not violate any HAL policies, does not perform illegal activities, and does not use the access for outside business interests. The HAL employee bears responsibility for the consequences should the access be misused.

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of HAL's network:

* Acceptable Encryption Policy
* Virtual Private Network (VPN) Policy
* Wireless Communications Policy
* Acceptable Use Policy

For additional information regarding HAL's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

## Specific Guidance

### Requirements

* Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
* At no time should any HAL employee provide their login or email password to anyone, not even family members.
* HAL employees and contractors with remote access privileges must ensure that their HAL-owned or personal computer or workstation, which is remotely connected to HAL's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
* HAL employees and contractors with remote access privileges to HAL's corporate network must not use non-HAL email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct HAL business, thereby ensuring that official business is never confused with personal business.
* Routers for dedicated ISDN lines configured for access to the HAL network must meet minimum authentication requirements of CHAP.
* Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
* Frame Relay must meet minimum authentication requirements of DLCI standards.
* Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.
* All hosts that are connected to HAL internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
* Personal equipment that is used to connect to HAL's networks must meet the requirements of HAL-owned equipment for remote access.
* Organizations or individuals who wish to implement non-standard Remote Access solutions to the HAL production network must obtain prior approval from Remote Access Services and InfoSec.

# Enforcement

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