# Document Control

## Versioning

|  |  |  |
| --- | --- | --- |
| **Name** | **Date** | **Reason** |
| Version 1 | February 1, 2019 | Placed into production |
| Version 1.1 | February 17, 2019 | Minor revision |

## 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 Corporate Policy Committee (CPC) at a minimum interval of quarterly (every 12 months) at a maximum interval of every 24 months.

### Previous Reviews

|  |  |  |
| --- | --- | --- |
| **Committee** | **Review Date** | **Approval Date** |
| CPC | 7/15/2018 | 8/1/2017 |
| CEO | 1/21/2019 | 1/22/2018 |

# Purpose

This document will identify elements of a good security policy, explain the need for information security, identify the information security roles and responsibilities, and establish minimum information security practices for Hierarchical Access Ltd’s computer resources and associated communication networks utilizing the Hierarchical Access Ltd enterprise network.

# 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 CEO with input from the HAL CIO and other members of management with an interest in the program.

# Roles & Responsibilities

## Overall Responsibility

The security of information assets at HAL is the primary responsibility of the CISO, who reports directly to the CIO with periodic briefings to the entire executive team. The CISO is responsible for the development of all HAL InfoSec policies, development and implementation of the risk management program, and all related training, practice, test and continuous improvement programs. The HAL CISO is also designated as the Corporate Change Control Manager (CCCM) responsible for controlling changes to HAL information assets and associated media.

## Sectional Responsibility

Each HAL branch office is expected to designate a local InfoSec manager, who will also serve as Regional Change Control officer (RCCO). This individual will ensure local InfoSec policies are in place, and in compliance with Corporate policies, as well as coordinate local risk management programs, and all regional training, practice, test and continuous improvement efforts.

## Employee Responsibility

Information security is the responsibility of every HAL employee that comes into contact with a HAL information asset, regardless of form or location. Every employee is expected to undergo annual InfoSec training, and compliance testing before being allowed to renew their credentials to HAL information assets. In addition, each department manager is responsible for the information assets of his or her department, and ensuring compliance with employee training and testing.

# Policy

## General Guidelines

Information security is defined as the protection of information and the systems and hardware that use, store, and transmit that information. Therefore, this policy is intended to give direction on accepted security practices designed to ensure information confidentiality, integrity, and availability of company assets by managing threats and reducing vulnerabilities.

Assets are defined, in this case, as items that are owned by the company, that have an assessed financial value. This would include computer hardware, software, information, and lines of communication coming into and leaving the company campus.

Threats are defined as objects, people, or other entities that represent a risk of loss to an asset(s). Threats occur in several categories. These include:

1. Acts of human error or failure (Accidents, employee mistakes)
2. Compromises to intellectual property (Piracy, copyright infringement)
3. Deliberate acts of espionage or trespass (Unauthorized access)
4. Deliberate acts of information extortion (Blackmail of disclosure)
5. Deliberate acts of sabotage or vandalism (Destruction of information)
6. Deliberate acts of theft (Illegal confiscation of equipment)
7. Deliberate software attacks (Viruses, worms, denial-of-service)
8. Deviations in QOS from service providers (Power and WAN issues)
9. Forces of nature (Fire, flood, earthquake, lightning)
10. Technical hardware failures or errors (Equipment failure)
11. Technical software failures or errors (Bugs, unknown loopholes)
12. Technical obsolescence (Antiquated or outdated technology)

Vulnerabilities are defined as weaknesses or faults in a system or protection mechanism that exposes information to an attack or damage. Attacks are acts of intentional or unintentional attempt to compromise the information and/or the systems that support it.

Hierarchical Access Ltd’s technology resources will proactively track threat activity and work to prohibit or correct such activity. Where unintentional unauthorized access is detected, the affected organization will be advised to correct exploitable vulnerabilities to prevent future occurrences. Where unauthorized access is determined to be intentional it will be assumed to be malicious and an appropriate response will be initiated.

All Hierarchical Access Ltd’s employees, contractors, agents or other individuals utilizing computer resources, data communication networks, or other information technology infrastructure resources owned or leased by Hierarchical Access Ltd, including any other state agencies having electrical connectivity to the network are subject to this policy.

Additionally, any remote access, such as dial up connections, personal Internet Service Provider access or VPN connection, onto the Hierarchical Access Ltd enterprise network or associated domains will have the same effect as direct access via HAL provided equipment or facilities.

## Specific Guidance

The continued use of information technology resources throughout Hierarchical Access Ltd’s working infrastructure has continued to evolve with the intent of improving services for our constituency. These improvements allow for rapid and efficient communication among various departments and often directly with the directors of the surrounding business community. Consequently, our constituency has become heavily dependent upon the availability of a reliable information technology infrastructure to meet its business needs. Unfortunately, the “electronic highways” that facilitate our ability to instantaneously share information also creates vulnerabilities, potentially allowing unauthorized persons to gain access to Hierarchical Access Ltd’s resources. In order to control threats to information technology resources across the enterprise network and associated domains, a series of Information security instructions, entitled “INFORMATION SECURITY POLICY, INSTRUCTIONS, AND TECHNICAL STANDARDS,” is established.

### Protection of Information:

Information must be protected in a manner commensurate with its sensitivity, value, and criticality

### Use of Information:

HAL computer and communications systems must be used for appropriate business purposes only, by authorized personnel.

### Information Handling, Access, & Usage:

All data and information sent over the HAL enterprise network, and associated domain communications systems, are the property of HAL.

### Data & Program Damage Disclaimers:

HAL is not held responsible for any loss or damage to data or software that results from its efforts to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems.

### Legal Conflicts:

HAL information security policies were drafted to meet or exceed existing federal and state laws and regulations. Any policy implemented by HAL that is found to be in conflict with any existing laws or regulations should immediately be brought to the attention of the HAL Information Security Officer

### Exceptions to Policies:

Exceptions to information security policies exist on occasion where a risk assessment examining the implications of being out of compliance has been performed, where a standard risk acceptance form has been prepared by the data owner or management, and where this form has been approved by both the HAL’s Information Security Officer and internal Audit Management.

### Non-enforcement:

Management’s non-enforcement of any policy requirement does not constitute its consent.

### Violation of the Law:

HAL will prosecute violators of federal and state computer crime laws as laid out within the applicable laws.

### Revocation of Access Privileges

HAL reserves the right to revoke a user’s information technology privileges at any time

### Industry-Specific Information Security Standards:

HAL information systems must employ industry specific information security standards

### Use of Information Security Policies and Procedures

All HAL information security documentation, including, but not limited to, policies, standards, and procedures, must be classified as “Internal Use Only”, unless expressly created for external business processes and partners.

### Authority Over Data:

HAL reserves the right to examine all information transmitted through these systems. Examination of such information may take place without prior warning to the parties sending or receiving such information.

### Expectation of Privacy:

Staff, contractors, agents or other individuals should have no expectation of privacy associated with the information they store in or send through these systems; most files and documents maintained by HAL are subject to public review under the Georgia Open Records Act. This includes computer files and other stored material regardless of the medium of storage.

### Mission Critical Systems Information Handling:

HAL reserves the right to delete, summarize, or edit any information posted to, or transiting through, HAL information systems. These systems are scarce, Company owned-resources designed to support mission critical Company activities and goals.

# 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 at the discretion of the Judges.*