# Document Control

## Versioning

|  |  |  |
| --- | --- | --- |
| **Name** | **Date** | **Reason** |
| Corp. CISO | 8/22/2018 | Initial Creation |
| Corp. CISO | 1/20/2019 | Changes |
|  |  |  |

## 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 | 1/21/2019 |
| Corporate CIO | 1/23/2019 | 1/23/2019 |

# 

# Purpose

The purpose of this policy is to provide guidance for how each branch will response to suspected incidents within the HAL organization on corporate owned systems and networks, where corporate owned is defined as any system operating in a HAL production environment on the company network, whether within the company owned facilities or issued to company agents or employees for use at remote locations for company business.

This policy seeks to minimize systems and networks disruption introduced by unauthorized activity and intrusions. It is management’s intent that improved communication and coordination be used to improve organizational response and mitigates damage from successful intrusions.

# 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 the CISO and other members of management with an interest in the program.

This policy is implemented by the HAL Incident Response Planning Team (IRPT). The IRPT is made up of the HAL CISO and representatives from each HAL division and regional office. The IRPT will meet from time to time as scheduled and to review and approve policy and procedure changes. The IRPT will approve modification using a simple voice vote with a majority consensus prevailing except that the CISO and the CIO each have the ability to veto any modification request. The CISO shall serve as the IRPT liaison to the Corporate Contingency Planning Management Team (CMPT).

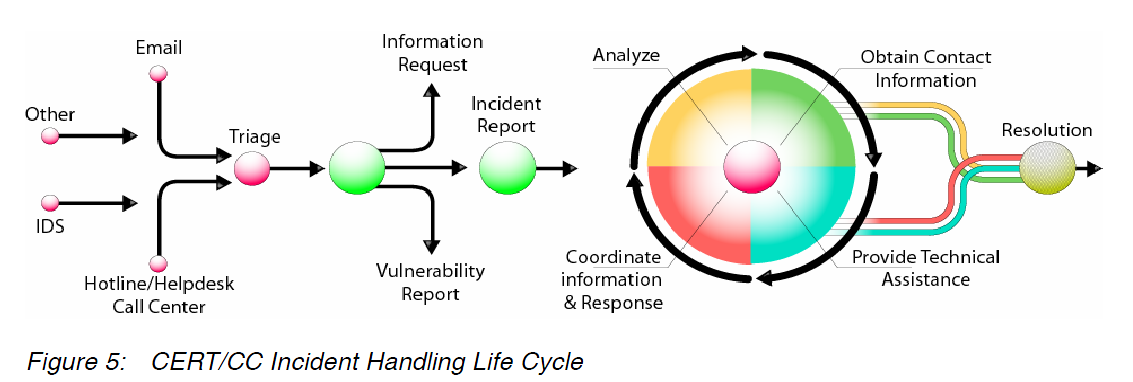
# Policy

## General Guidelines

For the purpose of this policy the following term will be used:

* Event – an activity or action within HAL systems or networks.
* Adverse Event – an event with the potential to negatively impact the confidentiality, integrity or availability of information stored, processed or transmitted through HAL systems or networks.
* Incident – An adverse event that has occurred, and actively threatens the security of information within HAL systems or networks.
* Intrusion – a penetration of HAL’s systems or networks by a threat. For HAL purposes the term incident will be used instead.
* Disaster – an incident which has escalated to the point where it threatens the continuity of operations of an entire branch, rather than just the security of information on HALs systems or networks.

HAL will use the CERT incident response methodology as follows:



(Source: Handbook for Computer Security Incident Response Teams) <http://www.cert.org/archive/pdf/csirt-handbook.pdf>)

As illustrated in the Figure above, a number of sources of information could indicate the presence of an incident as an adverse event in HAL’s systems or networks. Once an adverse event is reported, triage (assessment by a member of the CSIRT) will determine whether the adverse event is an actual incident. In the event it is determined to be an incident, the CSIRT assesses the severity and scope of the incident, and begins recording their initial findings using the HAL IR form.

The Team works to contain the incident as specified in the IR procedures documents. Once the incident has been contained, all systems recovered, and the vulnerability allowing the incident remediated, the CSIRT submits the IR form summarizing their findings, resolutions, and recommendations for changes to the IR procedures by email to [hal.ciso@seccdc.org](mailto:hal.ciso@seccdc.org) or [ciso@halcorp.biz](mailto:ciso@halcorp.biz), as appropriate.

## Specific Guidance

### Regional/Divisional Incident Response Planning Team Liaison

Each HAL Region or Division will appoint two team members as representatives to the corporate IRPT. These representatives may not include the Regional Manager (SECCDC Team Leader). It is strongly urged that both designated liaisons be identified and properly trained and kept current with ongoing issues.

### Change Management Documentation

All modifications to HALs systems in response to a documented incident are pre-approved under the provisions of the Emergency Change (Change Type 2) as per the Change Management Policy and Procedures. CSIRTs must coordinate with the regional Change Control Officer to ensure the proper documentation is completed and reported.

### IR Closure Reporting

Unless specified by the IR Procedure document, the CSIRT must resolve and report all incidents within three (3) hours of detection or risk administrative actions.

Complete and submit the IR Form, following all steps as outlined in the HAL IR Procedure.

### Incident to Disaster Escalation

The IR liaison to the Corporate IRPT will assess the incident during the response stage and determine whether the incident constitutes a real and present danger to the ongoing operations of the branch, based on the ability of the CSIRT to contain the incident. The liaison will notify the HAL CISO immediately should the team be unable to contain the incident. The CISO will make the final determination as to whether the incident has escalated to a disaster and will assign additional resources and make appropriate notifications as needed.

# Enforcement

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