# Document Change Control

## Versioning

|  |  |  |
| --- | --- | --- |
| **Name** | **Date** | **Reason** |
| Corp. Change Ctrl Officer | 8/22/2018 | Initial Creation |
| Corp. Change Ctrl Officer | 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 procedure is to provide guidance to all members of the HAL organization on how to implement the HAL Incident Response Policy.

# Scope

## Applicability

This procedure serves as a standard of performance and applies to all HAL employees and affiliates at all HAL facilities and locations world-wide.

## Ownership

This procedure is under the direct control of the HAL Corporate CISO with input from the CIO and other members of management with an interest in the program.

This procedure is promulgated by the HAL Incident Response Planning Team (hereafter IRPT) as defined in the HAL Incident Response Policy.

# Incident Response Process

## Incident Response Definitions

The incident response report form and how it is reported is defined in the HAL Policy for ISSP Incident Response.

## Initial IR Detection and Determination

Upon initial report from an outside or inside source, a member of the CSIRT will investigate the adverse event and determine if it is in fact an incident. The adverse event may be a detected external access attempt, or a discovered policy violation on HAL systems or networks. Upon incident declaration, the CSIRT will begin Incident Response activities to contain and recover from the incident.

### Initiating the IR Report Form

All detected incidents, regardless of type or origin, will be reported using the IR Report Form. Carefully read and follow the directions embedded in the IR Report Form as to how to complete all of the fields found in the document. Note that a separate report form will be filed for each incident detected by the CSIRT. Teams will begin completing the IR report form, documenting activities and observations. Additional information will be collected and entered in later stages of IR.

## Incident Containment and Recovery

Once the incident is detected, the CSIRT will take all reasonable and prudent steps to prevent the incident from doing any additional damage, and to restore controls over the systems. Some containment procedures could include:

* Disabling compromised user accounts
* Reconfiguring a firewall to block the problem traffic
* Temporarily disabling the compromised process or service
* Taking down the conduit application or server—for example, the e-mail server
* Stopping all computers and network devices

The CISRT will only take those steps necessary to regain control of HAL systems and networks, minimizing the disruption of HAL services and business functions. Once the incident is contained, the CSIRT will work to document the incident, and the extent of the damage resulting from the incident. Next the CSIRT will work to quickly and effectively remove all traces of the incident, restoring all systems and services to normal operation. All incidents must be resolved and reported within three (3) hours of detection, otherwise management will instigate administrative actions.

### Change Control Documentation

All changes to HAL systems and networks resulting from documented and established IR functions are pre-approved under the emergency provisions (Change Class Type 2) of the HAL Change Management Policy and Procedures.

As soon as the CSIRT regains control of HAL systems and begins to re-establish operations, the branch Change Control Officer should be notified so that he or she may begin documenting the changes resulting from the detection and resolution of the incident. All paperwork and approvals associated with the Change Management procedures must be fully complied with.

For all emergency change, the roll back portion of the CM form must provide a business-driven statement to justify the emergency change. If not completed, the request will face likely penalties.

### IR Reporting

Once the CSIRT declares the incident resolved, and all systems returned to normal, the team must complete and submit the IR Report Form. The form must be completely filled out and submitted to the CISO within three (3) hours of the detection of the incident.

The IR Report Form will be submitted via email to [hal.ciso@seccdc.org](mailto:hal.ciso@seccdc.org) or [ciso@halcorp.biz](mailto:ciso@halcorp.biz), as appropriate, and copied to the CISO.

# Enforcement

Any employee found to be in violation this policy may be subject to disciplinary action, up to and including termination of employment. Teams not submitting IR Report forms within three (3) hours of the detection of an incident may suffer administrative actions.

*NOTE: As part of the SECCDC event all red team actions and some systems MAY have a direct impact on the operations and services of the team. Successful detection, prevention and resolution of these incidents, accompanied by accurate reporting MAY mitigate up to 50 percent of the penalties associated with these actions.*