




HARRIS

HARRIS COMPUTER SYSTEMS CORPORATE CHANGE CONTROL POLICY

Corporate Officer: Dwayne Martin, Vice President of CIT

Signature: 

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	1/5/16	Gina Martin/Katie Rose	Major	Initial version of policy.	Todd Richardson
1.1	2/17/16	Katie Rose	Major	Responsibilities were changed from the Security Officer to the Change Manager. Added CAB information and introduced the Change Management Protocol.	Dwayne Martin
1.2	8/8/16	Gina Martin/Katie Rose	Minor	Final review and acceptance of revisions on 2/17/16.	Dwayne Martin
1.3	10/13/16	Katie Rose	Minor	Revisions to remove procedures that are defined in the associated Protocol document.	Dwayne Martin
1.4	10/22/18	Katie Rose	Minor	Annual Review	Dwayne Martin
1.5	3/25/2020 *2019 review waived as approval for 2018 review cycle completed end of Q1 2019	Katie Rose	Minor	Annual Review	Dwayne Martin
1.6	3/24/2021	Katie Rose	Minor	Annual Review, Added Definitions Document	Dwayne Martin

POLICY

Harris Computer uses formal change control procedures when implementing changes to its information systems. A Change Request (CR) submitted via RemedyForce is required for any alteration to a Harris Computer's information systems, infrastructure, or applications and/or their configuration, other than basic administration tasks that do not affect the security, integrity or availability of the information systems. The only exception is while actively working to resolve a Priority 1 (P1) or Priority 2 (P2) incident.

When new systems are introduced or changes are to be made to existing systems, a process of documentation, specification, testing, quality control, and managed implementation will be followed. All such Changes will be documented and implemented in a manner to ensure that existing security and control procedures are not compromised.

The Change Manager is responsible for ensuring:

- a) all Changes are properly analyzed, documented and communicated to those impacted by, or involved in their execution.
- b) Changes are submitted by authorized users.
- c) details of all Changes are tracked and stored.
- d) a risk analysis is performed prior to implementation to determine the potential impact of and need for any Change.
- e) no Change is implemented without being properly planned, documented, reviewed, tested and approved.
- f) system documentation and policies are updated upon completion of each Change and outdated documentation and policies are archived.
- g) A copy of all Change requests submitted and their disposition.
- h) Documentation of the risk analysis and its result for each approved change request.
- i) Documentation of the implementation of the change and any associated audit logs.

The Change Implementer is responsible for ensuring:

- a) the Change is properly planned and tested.
- b) communication to the impacted customers.

- c) rollback or backout plan is defined.
- d) additional resources are coordinated.
- e) the CR -Change Request - is implemented and ended on schedule.
- f) any exceptions are promptly reported to the Change Manager.

The Change Advisory Board (CAB) is responsible for ensuring:

- a) CR's are reviewed for completeness.
- b) CR's are reviewed for conflict of other planned changes.
- c) customer notification has taken place.
- d) impact to integrity and availability is considered.
- e) a rollback plan is in place.
- f) the CR is necessary to meet business needs.
- g) CR's are approved in a timely manner and rejected as needed to protect the integrity and availability of systems and data.
- h) any documentation or policy associated with the changed system is updated.

DEFINITIONS

See attached policy definitions or [click here](#).

REGULATORY REFERENCES

45 C.F.R. § 164.308