# Information Security Standard – Configuration Management

## Policy Statement

This Standard supports the {Company} Information Security & Privacy Policy and outlines the configuration management controls to be implemented across all of {Company}’s production systems.

## Applicability

Compliance with the controls outlined in this document is mandatory for all {Company} employees, contractors, vendors, and guests.

## Non-compliance

Any instances of non-compliance with the controls outlined in this document should be reported following the procedures outlined in the Reporting Process.

## Scope

The requirements of this standard to all systems that store, process, or transmit {Company} information; or are used to connect to those systems that are used to store, process, or transmit {Company}’s information.

## Controls

CM-1. All management and maintenance of production systems shall be done programmatically via Puppet or Chef {Link to Puppet/Chef documentation}.

CM-2. Any changes to the standard configuration are treated as source code and must go through {Company}’s established change management, code reviewing processes, and approvals outlined in the Change Management in the Production Environment process.

CM-3. Change control is the process used to document and review any non-standard or cross-functional change made to {Company}’s infrastructure. Change control events are tracked in theChange Control JIRA project.

## Appendices

### Document Management

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Syltor Consulting | Version | 1.0 |
| Date Modified | 30 May 2019 | Approver |  |
| Last Reviewed |  | Reviewer(s) |  |
| Review Cycle | Annual | Next Review Date |  |