# Information Security Standard – Security Assessment

## Policy Statement

This Standard supports the {Company} Information Security & Privacy Policy and outlines the mandatory requirements for performing security assessments of {Company}’s 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

1. {Company} will perform annual risk assessments that conform to an accepted international standard, such as PCI-DSS, ISO/IEC 27005, NIST SP 800-30 or CMU-OCTAVE/OCTAVE ALLEGRO. These assessments shall be performed annually at a minimum and updated to reflect substantive changes to the environment throughout the year. The Head of Security is responsible for leading these assessments.
2. Annually, {Company} will contract with a reputable professional services firm to perform a ‘white-box’ penetration test of the {Company} platform. These tests shall attempt to gain access to the {Company} system by enumerating and attempting to exploit vulnerabilities in the platform, with the goal of obtaining Administrative credentials on the portal or shell access on a host.
3. {Company} will maintain a public bug bounty program that encourages researchers to test the platform and report their findings under responsible disclosure principles.
4. {Company} will retain an independent and accredited third-party assessor to perform compliance audits for PCI-DSS, SOC-2, and any other compliance regimes that {Company} conforms to. All testing will be performed in accordance with the rules outlined in the compliance regime.
5. All findings from any assessment, audit, or test will be validated by the {Company} Security, Operations, and Engineering teams before acceptance. All valid findings will be triaged and tracked according to {Company}’s standard engineering and operations on-call processes.
6. All third-party products and services leveraged by {Company} must be evaluated for conformance to {Company}’s Security Policy and supporting Standards by the Security team before being placed into production. The results of these assessments shall be incorporated into {Company}’s annual risk assessment.
7. At least once per quarter, the {Company} security team will validate control efficacy over the preceding 90 days. A report shall be prepared by the security team and presented to senior management outlining the company’s alignment to the defined security controls. At a minimum these reports should include conformance to the defined Change Control and Release (CCR) process, firewall and other security tool validation, validation of daily security review activities, any incident response activities that occurred, and validation of system conformance to defined standards. This review shall be accomplished by performing the following:

* Reviewing all Firewall changes that have occurred to ensure there is a corresponding and approved CCR ticket.
* Validating evidence of daily log reviews by security and operations staff to ensure that reviews have occured.
* Reviewing all security incident tickets and validating that lessons learned have been compiled, remediation tasks identified, triaged, and placed into JIRA.
* Reviewing a sample of CCR ticket and validating that they were properly categorized, approved, and implemented
* Reviewing {Insert CI/CD Tools} logs and configuration against inventory scans to validate that all production systems have been deployed and maintained using CI/CD tools.

If the above activities are performed as part of an annual PCI-DSS or SOC-2 audit, the findings from that report may be provided in lieu of a separate report for SA-7.

## Appendices

### Document Management

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Syltor Consulting | Version | 1.0 |
| Date Modified | 29 May 2019 | Approver |  |
| Last Reviewed |  | Reviewer(s) |  |
| Review Cycle | Annual | Next Review Date |  |