# Information Security Standard – System Integrity

## Policy Statement

This Standard supports the {Company} Information Security & Privacy Policy and outlines the mandatory physical and environmental controls to be implemented across all 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

PSEC-1 All production datacenters shall conform to the requirements of NIST sp800-53r4 Moderate, PCI-DSS 3.2 or SSAE16/ISAE3402 SOC2, Type II.

PSEC-2 Only those {Company} employees with a specific business requirement as part of their assigned duties shall be allowed access to {Company}’s production datacenter facilities. The list of those personnel who require such access shall be maintained by the manager of the Datacenter Ops team and reviewed at least quarterly.

## Appendices

### Document Management

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