# Information Security Standard – Information Classification

## Policy Statement

This Standard supports the {Company} Information Security & Privacy Policy and defines the classification scheme for {Company}’s information assets.

## 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.

## Categories

Information shall be categorized according to the impact to the company if the controls protecting the information or information system containing said information were to fail and result in a loss of any of the following:

* Confidentiality (inadvertent or unauthorized disclosure)
* Integrity (inadvertent or unauthorized modification)
* Availability (inadvertent or unauthorized removal/deletion)

Information should be categorized according to the highest level of risk across these three areas. As an example if it is acceptable for the information to have low availability and low confidentiality, but requires high confidentiality; the information should be classified as {Company} Confidential; and be protected with all appropriate controls. By default, all information is considered to be **{Company} - Public**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Categorization** | **Definition** | **Confidentiality** | **Integrity** | **Availability** | **Examples** |
| {Company} - Confidential | Information that is required by law or contract to have the highest level of controls.  Information that if disclosed, modified, or offline without authorization would materially affect {Company}’s business. | Information shall be stored in {Company} approved cloud provider or other {Company} controlled systems.  Information shall only be stored or transmitted in encrypted form, using 256-bit symmetric and 2048-bit asymmetric key length.  Two-factor authentication is required to access the information. | All changes to the data must be tracked  Validation that the information has not been modified must be provided through hashing or other automated means. | Any downtime must be scheduled in advance.  Uptime requirement = 99.9%  Information is replicated in real-time and backed-up at least nightly to a separate facility.  Backups are retained for 90 days hot, 12 months cold. | Authentication credentials  Financial account information  PII  ePHI  PCI |
| {Company} - Internal | Internal business information and working data.  Information that if disclosed, modified, or offline without authorization would moderately affect {Company}’s business. | Information shall be stored in {Company} approved cloud provider or other {Company} controlled systems.  Information shall only be stored or transmitted in encrypted form, using 256-bit symmetric and 2048-bit asymmetric key length.    Access to the information requires strong password authentication. | The data shall be stored in systems that automatically track revisions and allow for roll-back of changes. | Any downtime must be scheduled in advance.  Uptime requirement = 99%  Information is replicated in real-time and backed-up at least nightly to a separate facility. | Strategic documents  Financial information  Unreleased source code  Raw log files |
| {Company} - Public | Information that can be freely release to the public and made available on the Internet. | The information can be shared freely. | The information is free to be modified and used by others. | Any downtime must be scheduled in advance.  Uptime requirement = 99%  Information is replicated in real-time and backed-up at least nightly to a separate facility. | Architecture documents  Website content  Marketing collateral  Released source code |

## 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 |  |