# Information Security Standard – Definitions

## Policy Statement

This Standard supports the {Company} Information Security & Privacy Policy and defines terms and acronyms used throughout {Company}’s Information Security & Privacy Program.

### Applicability

N/A

### Definitions

**access control** - means to ensure that access to assets is authorized and restricted based on business and security requirements

**administrative account** - user or system account that has the ability to affect modify the security or privacy controls of an information system

**attack** - attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

**audit** - systematic, independent and documented process for obtaining evidence and evaluating it objectively to determine the extent to which defined criteria are fulfilled

**authentication** - provision of assurance that a claimed characteristic of an entity is correct

**authenticity** - property that an entity is what it is claims to be

**availability** - property of being accessible and usable upon demand by an authorized entity

**confidentiality** - property that information is not made available or disclosed to unauthorized individuals, entities, or processes

**control** - measure that is modifying risk

**control objective** - statement describing what is to be achieved as a result of implementing controls

**electronic Protected Health Information** (**ePHI) -** personal healthcare data subject to the Health Insurance Portability and Accountability Act (HIPAA) or equivalent regulation

**event** - occurrence or change of a particular set of circumstances

**information** - an asset that, like other important business assets, is essential to an organization’s business and consequently needs to be suitably protected. Information can be stored in many forms, including: digital form (e.g. data files stored on electronic or optical media), material form (e.g. on paper), as well as unrepresented information in the form of knowledge of the employees.

**information asset** - see information

**information processing facility**- any information processing system, service or infrastructure, or the physical location housing it

**information security event** - identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant

**information security incident** - single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

**information system** - a collection of software and hardware that stores or processes information assets

**internal user** - {Company} employee, vendor, contractor, temporary, intern, or other such individual authorized to act on behalf of the company when managing {Company}’s information

**non-production systems** - those systems, such as user workstations, test environments, staging, and lab hosts that do not directly support or provide services to the {Company}’s production system.

**non-repudiation** - ability to prove the occurrence of a claimed event or action and its originating entities

**payment card industry (PCI)** - credit card numbers, mag stripe data, CVV/CVC1/2 and other information subject to the PCI Data Security Standard (PCI-DSS)

**personally identifiable information (PII) -** information that can be used to identify a specific individual as defined by NIST sp800-122, EU 95/46/EC, California’s SB 1386, or similar

**platform or customer account** - administrative, system, or user account that is used by {Company}’s customers or clients to access and manage the information that their organization has placed on the {Company} platform

**policy** - intentions and direction of an organization as formally expressed by its top management

**production system -** those systems used to operate and provide the {Company} Open Data Cloud to customers and the public.

**public account** - non-privileged user account that is used by a member of the public to access and save views of publicly-available data that {Company} customers have placed on the {Company} platform.

**security incident -** any unauthorized event or activity taken by internal or external entities that may adversely affect the confidentiality, integrity, or availability of the {Company} platform.

**sensitive information -**  information rated as {Company} Confidential, including but not limited to PII, ePHI, PCI, authentication credentials, and Financial account information

**system account** - credential to be used solely by automated processes

**threat** - potential cause of an unwanted incident, which may result in harm to a system or organization

**unauthenticated user** - a user or system that has not authenticated to the information system

**vulnerability** - weakness of an asset or control that can be exploited by one or more threats

### Acronyms

|  |  |
| --- | --- |
| **2FA / MFA** | Two-Factor Authentication / Multi-Factor Authentication |
| **3PAO** | Third Party Assessment Organization |
| **ASV/QSV** | Authorized/Qualified Security Vendor |
| **ATO** | Authorization to Operate |
| **C2** | Command & Control |
| **CERT** | Computer Emergency Response Team |
| **CIA** | Confidentiality, Integrity, Availability |
| **CIS** | Center for Internet Security |
| **CMS** | Centers for Medicare & Medicaid Services |
| **COTS** | Commercial Off The Shelf |
| **CSRF** | Cross-Site Request Forgery |
| **CVE** | Common Vulnerabilities and Exposures |
| **CVSS** | Common Vulnerability Scoring System |
| **(D)DoS** | (Distributed) Denial of Service |
| **EMF** | Electro-Magnetic Field |
| **FedRAMP** | Federal Risk Assessment & Management Program |
| **FIPS** | Federal Information Processing Standards |
| **FISMA** | Federal Information Security Management Act |
| **GSA** | [Unites States] General Services Administration |
| **HHS** | [United States Department of] Health & Human Services |
| **HIPAA** | Health Insurance Portability & Accountability Act |
| **IoC** | Indicator of Compromise |
| **IR** | Incident Response |
| **ISCP** | Information Security Contingency Plan |
| **ISO 2700x / ISO27k** | International Organization for Standardization's series of standards for information security |
| **JAB** | Joint Authorization Board |
| **(N)IDS** | (Network) Intrusion Detection System |
| **NIST** | National Institute of Standards and Technology |
| **OPM** | [United States] Office of Personnel Management |
| **OWASP** | Open Web Application Security Project |
| **PCI-DSS** | Payment Card Industry - Data Security Standards |
| **PIA** | Privacy Impact Assessment |
| **PII** | Personally Identifying Information |
| **PKCS** | Public Key Cryptography Standards |
| **PKI** | Public Key Infrastructure |
| **PLA** | People's Liberation Army |
| **POAM** | Plan Of Action & Milestones |
| **PoC** | Proof of Concept |
| **PRC** | People’s Republic of China |
| **RoB** | Rules of Behavior |
| **RTFM** | Read The [super]FUN Manual |
| **SDD** | Security Design Document |
| **SIEM** | Security Information Event Management |
| **SOP** | Standard Operating Procedure |
| **SOR(N)** | System Of Record (Notice) |
| **SOX** | Sarbanes-Oxley Act |
| **(S)SDL** | (Secure) Software Development Lifecycle |
| **SSO** | Single Sign-On |
| **SSP** | System Security Plan |
| **STIG** | Security Technical Implementation Guide |
| **TTP** | Trusted Third Party |
| **US-CERT** | United States Computer Emergency Readiness Team |
| **XSS** | Cross-Site Scripting |

## 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 |  |