Michael Anthony Borchardt
Information Security: What is Information Security?

March 4th, 2024

Objective and Scope

The purpose of this Information Security document is to better understand what information security is, with context to the broader scope of information technology.

Foremost, this document is intended to be used by any personnel involved in the maintenance or overseeing of IT operations.

1. Introduction

The materials presented within the contents of this document have been collected from several sources across the Internet. These organizations include, but are not limited to, the Open Web Application Security Project (OWASP), the National Institute of Standards and Technology (NIST), the SANS Institute, and other recognized sources of industry best practices.

2. What is Information Security?

Information is often one of the most important assets an organization has. Organizations can classify information in a number of different ways, which will provide direction to other people about how to use this information. The details about how to handle information are discussed in an organization’s information classification and handling policy. This represents an integral piece of an organization’s overall security policy.

Thus, simply put, information is data. Data is collected by an organization from customers of an organization, and data is stored on some form of physical medium, such as a hard-disk drive (HDD) or solid-state drive (SSD).

However, the act of securing information is the process by which an organization maintains the confidentiality, integrity, and availability of their data. Information security is concerned with protecting information in all its forms, whether written, spoken, electronic, graphic, or using other methods of communication.

3. How is Information Labeled?

Data policies can dictate information be labeled in a number of ways. Oftentimes, information intended for the public will be denoted public by an organization. This is information that does not need to be kept internal, confidential, or secret.

Information that is defined as internal would be information that is to be used by members of the organization, such as contractors and service providers. Information of this classification is usually intended to only been seen by employees.

An organization may have confidential information, which is information that is only available to external audiences for business-related purposes. Furthermore, this type of information usually requires the signing of a nondisclosure agreement (NDA).

Specialized information or secret information may include intellectual property or proprietary methodologies. If disclosed, this type of information may cause damage to the organization’s competitive advantage. It is usually restricted to a

few people or departments within a company and is rarely disclosed outside the company.

4. What is the CIA Triad?

The CIA triad references the three terms confidentiality, integrity, and availability. With regards to information security, an organization should always try to protect the confidentiality of information. Thus, private information should remain private.

Integrity calls to assuring that data not be corrupted while in motion or at rest. Foremost, data has two states. Data can be in motion, and data can be in rest. When data is being transferred from one place to another, data is in motion. However, when data is in storage, the data is at rest. Integrity is the process of making sure that data has not been tampered with.

Availability is the process of making sure that data is available for those who have authorization to use it, when they need to use it.