Appendix A: Definitions

**Cloud Computing Application:** Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Common examples of cloud computing applications are Dropbox, Facebook, Google Drive, Salesforce, and Box.com.

**Confidential Information:** Confidential Information is information protected by statutes, regulations, (District/Organization) policies or contractual language. Information Owners may also designate Information as Confidential. Confidential Information is sensitive in nature, and access is restricted. Disclosure is limited to individuals on a “need-to-know” basis only. Disclosure to parties outside of (District/Organization) must be authorized by executive management, approved by the Director of Information Technology and/or General Counsel, or covered by a binding confidentiality agreement.

Examples of Confidential Information include:

* Customer data shared and/or collected during the course of a consulting engagement
* Financial information, including credit card and account numbers
* Social Security Numbers
* Personnel and/or payroll records
* Any Information identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction
* Any Information belonging to an (District/Organization) customer that may contain personally identifiable information
* Patent information

**Incident:** An incident can have one or more of the following definitions:

1. Violation of an explicit or implied (District/Organization) security policy
2. Attempts to gain unauthorized access to a (District/Organization) Information Resource
3. Denial of service to a (District/Organization) Information Resource
4. Unauthorized use of (District/Organization) Information Resources
5. Unauthorized modification of (District/Organization) information
6. Loss of (District/Organization) Confidential or Protected information

**Information Resource:** 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: hardware assets (e.g. workstation, server, laptop) 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 may be transmitted by various means including: courier, electronic or verbal communication. Whatever form information takes, or the means by which the information is transmitted, it always needs appropriate protection.

**Internal Information:** Internal Information is information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Internal Information is information that is restricted to personnel designated by (District/Organization), who have a legitimate business purpose for accessing such Information.

Examples of Internal Information include:

* Employment Information
* Business partner information where no more restrictive confidentiality agreement exists
* Internal directories and organization charts
* Planning documents

**Mobile Device**: Computing devices that are intended to be easily moved and/or carried for the convenience of the user, and to enable computing tasks without respect to location. Mobile devices include, but are not necessarily limited to mobile phones, smartphones, tablets, and laptops.

**Penetration Test**: A highly manual process that simulates a real-world attack situation with a goal of identifying how far an attacker would be able to penetrate into an environment.

**Personally-owned**: Systems and devices that were not purchased and are not owned by (District/Organization).

**Public Information:** Public Information is information that may or must be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public Information, while subject to (District/Organization) disclosure rules, is available to all (District/Organization) employees and all individuals or entities external to the corporation.

Examples of Public Information include:

* Publicly posted press releases
* Publicly available marketing materials
* Publicly posted job announcements

**Removable media:** Portable devices that can be used to copy, save, store, and/or move Information from one system to another. Removable media comes in various forms that include, but are not limited to, USB drives, flash drives, read/write CDs and DVDs, memory cards, external hard drives, and mobile phone storage.

**Vulnerability Scan**: A vulnerability scan is an automated tool run against external and internal network devices and servers, designed to expose potential vulnerabilities that could be found and exploited by malicious individuals.

Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version  | Modified Date | Approved Date | Author | Reason/Comments |
| 1.0.0 | August 2016 |  | SecurityStudio | Document Origination |
|  |  |  |  |  |
|  |  |  |  |  |