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 Microsoft Office 365, Dropbox, Facebook, Google Drive, Salesforce, and Box.com.

**Confidential Information:** Confidential Information is information protected by statutes, regulations, [Company] 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 [Company] 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 [Company] customer that may contain personally identifiable information
* Patent information

**Critical Vendor:** a vendor with a specialized skillset, mandatory safety certification or proprietary product whose discontinuation of service would have a significant negative impact on company’s operations.

**Impact**: The extent of the damages resulting from an adverse event (i.e. realized threat) affecting Company Information Resources.

**Incident:** A suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification or destruction of information; interference with Information Resources or operations; or a significant violation of policy.

An incident may have one or more of the following characteristics:

1. Violation of an explicit or implied [Company] security policy
2. Attempts to gain unauthorized access to a [Company] Information Resource
3. Denial of service to a [Company] Information Resource
4. Unauthorized use of [Company] Information Resources
5. Unauthorized modification of [Company] information
6. Loss of [Company] 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.

**Information Resource Custodian:** the person, department, or entity responsible for supporting and implementing controls over **Information Resources**. For more information, refer to the Information Classification and Management Policy.

**Information Resource Owner:** the person, department, or entity responsible for classifying and approving access to an **Information Resource**. For more information, refer to the Information Classification and Management Policy.

**Information Security:** the practice of protecting information by mitigating risks to the confidentiality, integrity, and availability of information by means of administrative, physical, and technical **security controls.**

**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 [Company], 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

**Jail Breaking:** (also known as ‘rooting’) the process of modifying a mobile device to remove restrictions imposed by the manufacturer or operator, e.g. to allow the installation of unauthorized software.

**Least Privilege:** in a computing environment, requires that every module (such as a process, user, or program) be restricted to access only the information and resources that are necessary for its intended purpose.

**Likelihood:** the chance of something happening. With respect to information security, the chance of a threat or negative impact happening.

**Mitigating Control:** Existing or potential controls to be implemented to reduce the impact or likelihood of the risk from occurring.

**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.

**Mobile Device Management (MDM):** security software used by the organization to monitor, manage, and secure **mobile devices**.

**Multi-factor authentication:** an authentication control requiring the use of two or more pieces of evidence to an authentication mechanism. This evidence generally consists of something you know (knowledge), something you have (possession), and or something you are (inherence). Examples include: a physical security key, digital security certificate, security token, fingerprint, or possession of a mobile device.

**Need to Know:** a term used to describe the restriction of data or systems which are considered very sensitive. “Need to know” is used to describe the requirement that a person have a legitimate purpose for accessing data or systems regardless of their clearance level or access permissions.

**Overwrite:** see Secure Erase.

**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 Identifiable Information (PII):** Any information that when used alone or with other relevant data can identify an individual. For example: full name, social security number, driver’s license number, passport number, bank account number.

**Personally owned**: Systems and devices that were not purchased and are not owned by [Company].

**Protected Health Information (PHI):** health information in any form, including physical records, electronic records, or spoken information which includes identifiers allowing it to be linked to a specific individual.

**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 [Company] disclosure rules, is available to all [Company] 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

**Remote wipe:** a security feature that allows a network administrator or device owner to send a command that deletes some or all data located on a computing device without having possession of it.

**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.

**Residual Risk:** risks or risk-level remaining after mitigating controls have been accounted for.

**Risk:** the likelihood and resulting impact of an adverse (harmful) event. Risk is sometimes noted as Likelihood x Impact of an adverse event. A higher Risk Level indicates a higher potential likelihood and impact to the organization. A lower Risk Level indicates a lower likelihood and impact.

**Risk Assessment:** a method of identifying and evaluating risks to the organization. A risk assessment typically identifies the applicable threats and vulnerabilities that exist (or could exist), compared with existing controls, to determine the potential likelihood and impact of an adverse event.

**Secure Erase:** more commonly referred to as a “wipe”, is a way to overwrite all existing data on a media device with at least one set of binary zeroes ( 0 ) or ones ( 1 ) so the data cannot be read.

**Security Awareness:** the knowledge and perception members of an organization possess regarding the protection of the physical and informational assets of that organization.

**Security Controls:** (also known as “Mitigating Controls”) safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

**Signature Card:** a document that a service provider keeps on file with the identity and/or signatures of all the authorized people on that account.

**Technical Controls:** See Security Controls.

**Threat**: any circumstance or event with the potential to cause harm to an **Information Resource** or the organization. Common threat-sources can be natural, human, or environmental.

Two-factor Authentication: a type, or subset, of multi-factor authentication, see definition above.

**Vulnerability**: a flaw or weaknesses that could be exploited or triggered by a potential **threat**.

**Vulnerability Scan**: 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 2020 |  | FRSecure | Document Origination |
|  |  |  |  |  |
|  |  |  |  |  |