Data Classification Policy

1. Purpose

The purpose of this policy is to establish a framework for classifying data based on its sensitivity, value and criticality to Les Poupées Russes. Classification of data will aid in determining baseline security controls for the protection of data.

2. Scope

This Policy applies to any form of data, including paper documents and digital data stored on any type of media. It applies to all of Les Poupées Russes employees, as well as to third-party agents authorized to access the data.

3. Roles and Responsibilities

Data owners — The person who is ultimately responsible for the data and information being collected, usually a member of senior management. They are responsible for decisions about the usage of Les Poupées Russes data under their purview.

Data users — Person, organization or entity that interacts with, accesses, uses or updates data for the purpose of performing a task authorized by the data owner. Data users must use data in a manner consistent with the purpose intended, and comply with this policy and all policies applicable to data use.

4. Data Classification

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to Les Poupées Russes should that data be disclosed, altered, or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All company data should be classified into one of three sensitivity levels, or classifications:

Restricted Data — Data should be classified as Restricted when the unauthorized disclosure, alteration, or destruction of that data could cause a significant level of risk to Les Poupées Russes or its affiliates. Examples of Restricted Data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted Data.

Private Data — Data should be classified as Private when the unauthorized disclosure, alteration, or destruction of that data could result in a moderate level of risk to Les Poupées Russes or its affiliates. By default, all data that is not explicitly classified as Restricted or Public Data should be treated as Private Data. A reasonable level of security controls should be applied to Private Data.

Public Data — Data should be classified as Public when the unauthorized disclosure, alteration, or destruction of that data would result in little or no risk to Les Poupées Russes and its affiliates. Examples of Public Data include press releases, course information, and research publications. While little or no controls are required to protect the confidentiality of Public Data, some level of control is required to prevent unauthorized modification or destruction of Public Data.

An appropriate Data Owner should perform classification of data.

A. Data Collections

Data Owners may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data

collection consists of a user's name, address and social security number, the data collection should be classified as Restricted even though the user' name and address may be considered Public Information.

B. Reclassification

On a periodic basis, it is important to reevaluate the classification of data to ensure the assigned classification is still appropriate based on changes to legal and contractual obligations as well as changes in the use of the data or its value to Les Poupées Russes. The appropriate Data Owner should conduct this evaluation. Conducting an evaluation on an annual basis is encouraged; however, the Data Owner should determine what frequency is most appropriate based on available resources. If a Data Owner determines that the classification of a certain data set has changed, an analysis of security controls should be performed to determine whether existing controls are consistent with the new classification. If gaps are found in existing security controls, they should be corrected in a timely manner, commensurate with the level of risk presented by the gaps.

C. Calculating Classification

In some situations, the appropriate classification may be more obvious, such as when federal laws require Les Poupées Russes to protect certain types of data (e.g., personally identifiable information). If the appropriate classification is not inherently obvious, consider each security objective using the following table as a guide.

C.1. Confidentiality

Restrict access to and disclosure of data to authorized users in order to protect personal privacy and secure proprietary information.

Low impact: Unauthorized disclosure of the information is expected to have limited adverse effects on operations, organizational assets, or individuals.

Moderate impact: Unauthorized disclosure of the information is expected to have a serious adverse effect on operations, organizational assets, or individuals.

High impact: Unauthorized disclosure of the information is expected to have a severe or catastrophic adverse effect on operations, organizational assets, or individuals.

C.2. Integrity

Guard against improper modification or destruction of data, which includes ensuring information nonrepudiation and authenticity.

Low impact: Unauthorized modification or destruction of the information is expected to have a limited adverse effect on operations, assets, or individuals.

Moderate impact: Unauthorized modification or destruction of the information is expected to have a serious adverse effect on operations, assets, or individuals.

High impact: Unauthorized modification or destruction of the information is expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.

C.3. Availability

Ensure timely and reliable access to and use of information.

Low impact: Disruption of access to or use of the information or information system is expected to have a limited adverse effect on operations, assets, or individuals.

Moderate impact: Disruption of access to or use of the information or information system is expected to have a serious adverse effect on operations, assets, or individuals.

High impact: Disruption of access to or use of the information or information system is expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.

D. Predefined Types of Restricted Information

D.1. Authentication Verifier

An Authentication Verifier is a piece of information that is held in confidence by an individual and used to prove that the person is who they say they are. In some rare instances, an Authentication Verifier may be shared amongst a small group of individuals. An Authentication Verifier may also be used to prove the identity of a system or service. Examples include, but are not limited to: Passwords, Shared secrets, Cryptographic private keys.

D.2. Payment Card Information

Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements: Cardholder name, Service code, Expiration date, CVC2, CVV2 or CID value, PIN or PIN block, Contents of a credit card's magnetic stripe.

D.3. Personally Identifiable Information ("PII")

For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements: Social security number, Driver's license number, Identification card number, Financial account number in combination with a security code, access code or password that would permit access to the account, Medical and/or health insurance information.

D.4. Protected Health Information ("PHI")

PHI is defined as "individually identifiable health information" transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium. PHI is considered individually identifiable if it contains one or more of the following identifiers: Name, Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code), All elements of dates (except year) related to an individual (including birth date, admissions date, discharge date, date of death and exact age if over 89), Telephone numbers, Fax numbers, Electronic mail addresses, Social security numbers, Medical record numbers, Health plan beneficiary numbers, Account numbers, Certificate/license numbers, Vehicle identifiers and serial numbers, including license plate number, Device identifiers and serial numbers, Universal Resource Locators (URLs), Internet protocol (IP) addresses, Biometric identifiers, including finger and voice prints, Full face photographic images and any comparable images, Any other unique identifying number, characteristic or code that could identify an individual.

5. Revision History

1.0 Date of change: 01/12/2019 - Responsible: Technical team - Summary of Change: Initial release