Data Classification and Handling

Policy Statement

Accidental, unauthorized disclosure, theft, and dissemination are among the risks involved in handling sensitive information. This policy establishes Castle's data classification and handling scheme, and provides direction as to the appropriate handling of such information.

Scope: this policy applies to the entire Castle organization, as well as anyone otherwise having access to Castle sensitive information, and is part of the Castle corporate information security policy.

Introduction

Castle's data classification system has been designed to support the "need to know" so that information will be protected from unauthorized disclosure, use, modification, and deletion. Consistent use of this system will facilitate business activities and help reduce associated costs. Castle otherwise risks loss of customer relationships and public confidence, operational disruption, excessive costs, and ultimately suffering a competitive disadvantage.

Consistent Protection: Information must be consistently protected throughout its life cycle, from its origination to its destruction. Information must be protected in a manner commensurate with its sensitivity, no matter where it resides, what form it takes, what technology is used to handle it, and what purpose(s) it serves. Although this policy provides overall guidance, to achieve consistent information protection, employees will be expected to apply and extend these concepts to fit the needs of day-to-day operations.

Applicability: This policy is applicable to all information in Castle's possession or under Castle's control. For example, sensitive information entrusted to Castle by consumers, suppliers, business partners, and others must be protected according to this policy. Employees are expected to protect third party information with the same care that they protect Castle information.

No distinction is made between the words "data" and "information" for the purposes of this policy.

Classification Levels and Definitions

All data must be classified with one of the following four classification levels:

SECRET: This classification applies to the most sensitive business information within Castle. Its unauthorized disclosure could have material negative impact on Castle, its business partners, vendors or customers. Examples include merger and acquisition documents, corporate strategic plans, litigation strategy memos, and trade secrets. Access to such information is expected to be strictly limited to a specific set of Castle personnel.

CONFIDENTIAL: This classification applies to less sensitive business information that is intended for use within Castle. Its unauthorized disclosure could adversely impact Castle, employees, business partners, vendors or customers. Information that some people would consider to be private is included in this classification. Examples include employee performance evaluations, consumer Privately Identifiable Information (PII), PCI and other financial data, passwords, and internal audit reports.

INTERNAL USE ONLY: This classification applies to all other Castle information that does not clearly fit

into the above two classifications. While its unauthorized disclosure is against policy, it is not expected to have a significant adverse impact on Castle, employees, business partners, vendors or customers. Most Castle information falls within this category.

PUBLIC: This classification applies to information that has been explicitly approved by Castle for public release. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm. Examples include product brochures, advertisements, job opening announcements, and press releases.

Sensitive Information: Information is deemed sensitive if it is classified as confidential or secret. To assist in reading this policy, clauses pertaining only to sensitive information are highlighted. This policy further ends with a section with specific, additional recommendations for handling secret information.

Access and Communications

Need to Know: Information should be disclosed only to those people who have a legitimate business need for it. This principle applies to sensitive information such as source code, litigation strategy and credit card transaction data, just as it applies to internal information such as marketing research.

Restricted Downgrading: employees must not reclassify information to a lower sensitivity level unless this action is formally approved by the information owner.

System Access Controls: All sensitive information must be protected via access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable. Access control systems must allow access based on need to know, and log which users accessed which sensitive data at what time.

Access Granting Decisions: Access to Castle sensitive information must be provided only after express authorization of the information owner has been obtained. Custodians of the involved information must refer all requests for access to information owners.

Public Transmission: If Castle sensitive data is transmitted over any publicly accessible communication network, it must be encrypted, and only using strong encryption (e.g. TLS 1.2+).

Information Ownership

Production Information: All production information must have a designated information owner. Production information is information routinely used to accomplish business objectives. Examples include payroll summaries, shipping schedules, and managerial cost accounting reports, as well as customer data in Castle's cloud service environment. Information owners are responsible for assigning appropriate sensitivity classifications.

Access Decisions: Information Owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. Information owners must additionally take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and usage of information.

Labeling

What Gets Labeled (Default Classification): The vast majority of Castle information falls into the *Internal Use Only* category. For this reason, it is not necessary to apply a label to such information. Information without a label is therefore by default classified as *Internal Use Only*.

Information Collections: employees who create or update a collection of information are responsible for choosing an appropriate data classification label for the new or updated collection. This label must be consistent with the decisions made by the relevant information owners and should generally be the highest classification level found in the collection. Examples of such collections include databases, management reports, and Amazon AWS S3 buckets.

Third Party Information Labels: All externally provided information which is not clearly in the public domain must be classified by Castle. If not otherwise identified as sensitive by its source, it may be considered as Internal Use Only.

Consistent Labeling: sensitive information, from the time it is created until it is destroyed or declassified, it must be labeled (marked) with an appropriate data classification designation. Labels must appear on all manifestations of the information, electronic or hardcopy.

Sensitive Hardcopy: All printed, handwritten, or other paper manifestations of sensitive information must have a clearly evident classification label on each page. If bound, all sensitive information hardcopy must have an appropriate sensitivity label on the front cover and/or title page. The cover sheet for faxes containing sensitive information must also contain the appropriate classification label.

Removable Storage Media: If sensitive information is recorded on removable electronic storage media, it must be encrypted, and protected by proper access controls.

Third Party Interactions

Third Parties Need to Know: Unless designated as public, all Castle internal information must be protected from disclosure to third parties. Third parties may be given access to Castle internal information only when a demonstrable need-to-know exists, and when such disclosure has been expressly authorized by the relevant Castle information owner. All disclosures of sensitive Castle information to third parties must be accompanied with a signed non-disclosure agreement (NDA). Such disclosures must be accompanied by a log (e.g. email trail) indicating what information was provided, when, and to whom.

Third Party NDAs: When representing Castle, employees must not sign third party NDAs without advance authorization from Castle legal counsel.

Third Party Requests: Unless a worker has been authorized by the information owner to make public disclosures of nonpublic information, all requests for information about Castle and its business must be referred to a company executive or public relations. Such requests include questionnaires, surveys, newspaper interviews, and the like.

Prior Review: Every speech, presentation, technical paper, book, or other communication to be delivered to the public in representation of Castle must first have been approved for release by the involved employee's immediate manager.

Information Owner Notification: If sensitive information is lost, is disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, its owner must be notified immediately.

Shipping and Handling

Outside Services: Prior to sending any sensitive information to a third party for copying, printing, formatting, or other handling, the third party must sign a Castle NDA.

Page Numbering: All sensitive Castle information in paper form must indicate both the current and the last page numbers ("Page X of Y").

Backup Media: To prevent it from being revealed to or used by unauthorized parties, all sensitive information recorded on removable computer media (tapes, DVDs, USB keys, etc.) and stored outside Castle offices must be encrypted, with encryption keys stored safely in a manner approved by the CISO.

Envelopes: If sensitive information is to be sent through external mail or by courier it must be enclosed in a sealed, opaque, secured envelope or container. The envelope or container must not indicate the classification of the nature of the information contained therein. All envelopes or containers containing sensitive information must always be addressed to a specific person, and must also contain sufficient return address information.

Delivery of Hardcopy: Sensitive information in hardcopy must be personally delivered to the designated recipients, not to an unattended desk nor left out in the open. Alternatively, it may be made available to designated recipients via locked cabinets or similar physical security methods.

Declassification/Downgrading

Notifications: The information owner may, at any time, declassify or downgrade the sensitivity classification of their information. To achieve this, they must: (1) change the classification label appearing on the original document, and (2) notify all known recipients.

Reclassification Dates: If known in advance, the date that sensitive information will no longer be sensitive (declassified) must be indicated on all Castle sensitive information.

Destruction and Disposal

Destruction Approval: employees must not destroy or dispose of potentially important Castle records or information without specific advance management approval. Records and information must be retained if: (1) they are likely to be needed in the future, (2) regulation or statute requires their retention, or (3) they are likely to be needed for the investigation or prosecution of unauthorized, illegal, or abusive acts.

Default Retention Periods: All sensitive Castle information must be destroyed or disposed of when no longer needed. Information owners must review the schedule issued by the legal department to determine the minimum legal periods that information must be retained.

Destruction Methods: All sensitive information no longer in use may be placed in designated locked

boxes until authorized Castle personnel or a bonded destruction service pick it up. Otherwise, sensitive information in hardcopy must be cross-shredded or incinerated, while such information in other forms must be delivered to the IT department for secure destruction.

Physical Security

Office Access: Access to every office, conference room, and work area containing sensitive information must be physically restricted, with an appropriate access control method (receptionists, key cards, locks, biometrics, etc.).

Locked Containers: Secret information in hardcopy must be locked up when not actively in use, even if it is within an access-controlled building. If not encrypted, all secret information must be locked in safes, heavy furniture, or other containers approved by the IT department. It is advised to handle other sensitive information in the same manner.

Special Considerations and Recommendations for Handling Secret Information

Numbering Copies: All copies of secret documents should be individually numbered, and also include the label "Do Not Copy Without Explicit Permission from <name of information owner>."

Making Copies: Making or printing additional copies of secret information should not occur without the explicit permission of the information owner. If a copier or printer malfunctions when making copies of secret information, the involved employees should not leave the machine until all copies of secret information are removed from the machine and destroyed.

Logs: When secret information is involved, the information owner should keep a log reflecting the number of copies made, and when they were made.

Couriers: Secret information in hardcopy should only be sent by bonded courier or registered mail, and all deliveries should require acknowledgment of receipt from the intended recipient.

Transporting Secret Information: employees in the possession of smartphones, laptops, tablets, and other mobile devices containing secret Castle information should not leave them unattended at any time unless the secret information has been encrypted. Likewise, if secret data is to be transported in removable media (e.g. USB keys, DVDs), it should also be encrypted. Secret hardcopy should not be left unattended in a vehicle, hotel room, office, or other location, and should be carried at all times instead.

Viewing in Public: employees should avoid viewing secret information on public transportation. Easily assimilated secret information should not be read, discussed, or otherwise exposed on airplanes, restaurants, elevators, restrooms, or other public places where it could be overheard.

Storage: Electronic secret information should be encrypted when not in active use.

Speakerphones: Secret information should not be discussed on speakerphones unless all participating parties first acknowledge that no unauthorized persons are in close proximity such that they might

overhear the conversation. To help ensure that the information is communicated only to the intended party, employees should refrain from leaving messages containing secret information on answering machines or voicemail system.

Transmission Encryption: Secret information should always be encrypted in transmission, even over internal, private networks.