Custom Catch Data Governance Policy

PURPOSE

Custom Catch and partner data are assets maintained to support Custom Catch’s central missions of selling customized products, and providing customer service to support those sales. "Custom Catch data" refers to collections of data elements relevant to the operations, planning, or management of any unit at Custom Catch, or data that are reported or used in company reports. To support effective operations, Custom Catch data and partner data must be accessible for the purpose intended and only the purpose intended in completing its missions.

The purpose of data governance is to develop company policies and procedures that ensure that Custom Catch data meet these criteria within and across Custom Catch’s data systems, particularly the order fulfillment and messaging systems.

The purpose of the current Data Governance Policy is to achieve the following:

- Establish appropriate responsibility for the management of Custom Catch data and partner data as a company asset.

- Ensure data is used protected and used only for the purpose of meeting fulfillment and service needs for which it is intended

- Improve the security of the data, including confidentiality and protection from loss. Improve the integrity of the data, resulting in greater accuracy, timeliness, and quality of information for decision-making. The Data Governance Policy addresses data governance structure and includes policies on data access, data usage, and data integrity and integration.

ENTITIES AFFECTED BY THIS POLICY

Anyone at Custom Catch who creates data, accesses data or manages it, or relies on it for decision making and planning.

WHO SHOULD READ THIS POLICY

Data governance executive sponsors, data stewards, and all other Custom Catch employees who use data, regardless of the form of storage or presentation.

POLICY

Table of Contents

Data Governance Structure

Data Governance is the practice of making strategic and effective decisions regarding Custom Catch's information assets and information assets of Custom Catch partners. It assumes a philosophy of restricted access to Custom Catch data by all members of the company coupled with the responsibility to adhere to all policies and all legal constraints that govern that use. In the interest of attaining effective data governance, the company applies formal guidelines to manage the company's information assets and assigns roles to implement them. While the company data administrator is assigned a leadership role and oversight for the activities of data governance, this function is shared among the executive sponsors, data stewards, data administrators, and data users. Executive sponsors will appoint data stewards, and through the establishment of data policies and company priorities, provide direction to them and data administrators. The company's data stewards comprise the Data Governance Council, a body that meets regularly to address a variety of data issues and concerns

Overview of Roles for Governing Custom Catch data

The following are general descriptions of the primary roles and responsibilities within Data Governance.

Executive Sponsors

Executive sponsors are senior company officials who have planning and policy responsibility and accountability for major administrative data systems within their functional areas. By understanding the planning needs of the institution, they are able to anticipate how data will be used to meet company needs. Executive sponsors include the following administrative personnel currently in place at Custom Catch: Don MacFadyen, Donna MacFadyen. Executive sponsors meet as a group regularly to address a variety of data issues and concerns.

Director of Data Management

The director of data management, Don MacFadyen, works with the company needs to define a companywide structure of data stewardship by making explicit the roles and responsibilities associated with data management and compliance monitoring. This individual is responsible for coordinating data policies and procedures in all company data systems – sales, fulfillment and finance information systems in particular- ensuring representation of the interests of data stewards, managers, and key users. The director of data management coordinates the meetings and agendas for the executive sponsors and Data Governance Council and provides support to related data management efforts. This individual is also responsible for developing a company culture that supports data governance in areas with critical information. Informed by the Data Governance Council, the data administration area, led by the director of data management, is responsible for developing the company data structures and protection mechanisms.

Data Stewards

Data stewards are appointed by executive sponsors to implement established data policies and general administrative data security policies. Data stewards, who comprise the Data Governance Council, are responsible for safeguarding data from unauthorized access and abuse through established procedures and educational programs. They authorize the use of data within their functional areas and monitor this use to verify appropriate data access. They support access by providing appropriate documentation and training to support company data users. The role of Data Steward is filled by Don MacFadyen.

Data Administrators

Data administrators are company employees who most often report to data stewards and whose duties provide them with an intricate understanding of the data in their area. They work with the data stewards to establish procedures for the responsible management of data, including data entry and reporting. Some data administrators may work in a technology unit outside of the functional unit, but have responsibilities for implementing the decisions of the stewards. Technical data administrators are responsible for implementing backup and retention plans, or ensuring proper performance of database software and hardware. The role of Data Administrator is filled by Don MacFadyen.

Data Access Policy

The purpose of the data access policy is to ensure that employees have appropriate access to operational information, while recognizing the company's highest priority and responsibility for the security of data. The procedures established to protect that data must not be compromised for business efficiency. This policy applies to all uses of company and partner data, regardless of the function the data provides or the format in which the data reside.

Statement of Policy

The value of data as a company resource is increased through its widespread and appropriate use; its value is diminished through misuse or misinterpretation. The company will protect its data assets through security measures that assure the proper use of the data when accessed. Every data item will be classified by the relevant data steward to have an appropriate access level. Data access will be conducted in accordance with the policies established by the Director of Data Management. Any employee requiring access to company data will need to have approval to access the specific granular data element that they require to accomplish the duties of their position.

Data Usage Policy

The purpose of the data usage policy is to ensure that company data are not misused or abused, and are used ethically, according to any applicable law, and with the highest consideration for individual privacy. Use of data depends on the security levels assigned by the data steward.

Statement of Policy

Company personnel must access and use data only as required for the performance of their job functions, not for personal gain or for other inappropriate purposes; they must also access and use data according to the security levels assigned to the data. Data usage falls into the categories of update, read-only, and external dissemination.

Authority to update data shall be granted by the appropriate data steward only to personnel whose job duties specify and require responsibility for data update. This restriction is not to be interpreted as a mandate to limit update authority to members of any specific group, but should be tempered with the company's desire to provide excellent service to customers and partners.

Read-only usage to administrative summary information will be provided to employees for the support of company business without undue restrictions.

No company data is approved for public dissemination without specific approval of each data element by the Director of Data Management. All data usage will be conducted in accordance with policies established by the Director of Data Management.

Consequence of Noncompliance with Data Usage Policy

Company employees who fail to comply with the data usage policy will be considered in violation of the relevant company codes of conduct and will be subject to disciplinary action (up to and including termination of employment) or to legal action if laws have been violated. In less serious cases, failure to comply with this policy could result in denial of access to company data

Data Integrity and Integration Policy

The purpose of this policy is to ensure that company data have a high degree of integrity and that key data elements can be integrated across applications and electronic systems so that company staff, and management may rely on data for information and decision support.

Data integrity refers to the validity, reliability, and accuracy of data. Data integrity relies on a clear understanding of the business processes underlying the data and the consistent definition of each data element.

Data integration, or the ability of data to be assimilated across information systems, is contingent upon the integrity of data and the development of a data model, corresponding data structures, and domains.

Statement of Policy

Company data will be consistently interpreted across all systems according to the best practices agreed upon by the Data Governance Council, and it will have documented values in all company systems. Data administration will ensure that the needs of users of company data are taken into consideration in the development and modification of data structures, domains, and values. It is the responsibility of each data steward to ensure the correctness of the data values for the elements within their charge and the classification of data elements for protection based on the sensitivity of the information and whether Personally Identifiable Information is included in the information. Any data values, whether internal data or partner data, that contain Personally Identifiable Information are considered to require the highest level of data protection and security.

Company data are defined as data that are maintained in support of a group's operation and meet one or more of the following criteria:

- the data elements are key fields, that is, integration of information requires the data element;
- the company must ensure the integrity of the data to comply with company reporting requirements, including company planning efforts;
- the data are reported on or used in official company reports;
- a variety of users require the data.

It is the responsibility of each data steward, in conjunction with the Data Governance Council, to determine which core data elements are part of company data.

Documentation (metadata) on each data element will be maintained within a company repository according to specifications provided by the Director of Data Management and informed by the Data Governance Council. These specifications will include both the technical representation/definition of each element, as well as a complete interpretation that explains the meaning of the element and how it is derived and used. The interpretation will include acceptable values for each element, and any special considerations, such as if the data element is personally identifiable information.

All employees are expected to bring data problems and suggestions for improvements to the attention of the appropriate data stewards, the Data Governance Council, or the director of data management.