Data Governance Policy for the East Kingdom Webministry

Purpose

Data policies are a collection of principles that describe the rules to control the integrity, security, quality, and usage of data during its lifecycle. The purpose of this policy is to:

- Define East Kingdom Webministry data
- Establish clear lines of accountability
- Develop best practices for data management and protection

Scope

This policy applies to data collected, stored, archived, maintained, or in any way under the management of the East Kingdom Webministry, whether stored on Kingdom owned systems or within a third-party service, and it applies to all those who use this data.

This policy establishes the rules, roles, and responsibilities related to the management, including acquisition, utilization, maintenance, access and protection, of East Kingdom Webministry data.

This policy creates technical and behavioral standards and guidelines in creation and management of East Kingdom Webministry data, as related to data quality and consistency, security and privacy, compliance, retention and archiving, and access by individuals.

Classifications of Data

Regulated Data

Information that if disclosed or modified without authorization would have severe adverse effects on the operations, assets, or reputation of the East Kingdom, or the East Kingdom Webministry obligations concerning information privacy. In general, information in the Regulated Data class is subject to extensive, specific security and privacy regulations.

Regulated Data includes data that is protected by international, federal or state laws or regulations. Information protected by these laws includes, but is not limited to, Personally Identifiable Information, Nonpublic Personal Information, and Personal Health Information.

Restricted Data

Information that if disclosed or modified without authorization would have severe adverse effects on the operations, assets, or reputation of the East Kingdom, or the East Kingdom Webministry obligations concerning information privacy, but is not governed by external law or regulation.

Restricted data includes, but is not limited to, kingdom financial records, and information related to legal or disciplinary matters. Credentials such as passwords or passphrases are included in this class.

Confidential Data

Information that if disclosed or modified without authorization would have moderate adverse effects on the operations, assets, or reputation of the East Kingdom, or the East Kingdom Webministry obligations concerning information privacy. This class of data also includes data the Webministry has chosen to treat confidentially for Webministry business.

Public Data

Information that poses little or no risk to individuals and to the East Kingdom. The data is accessible without limitation to anyone regardless of institutional affiliation. It may be freely used, reused and reattributed.

Data Trustees

Data Trustees are the Greater and Lesser Officers of the East Kingdom. They provide a strategic perspective on data governance. They have decision-making authority regarding East Kingdom data maintained and managed by the Data Stewards and Custodians. They have the primary responsibility to ensure that the Webministry, and the officers in their own offices, are following Data Governance Policies and are in compliance with Society guidelines and federal and state laws and regulations. They identify the data classification (sensitivity) of data governed or managed by their respective offices. Data Trustees are responsible for engaging affected offices and the user community before formulating changes or additions to this Data Governance Policy.

Data Stewards

Data Stewards, assigned by the Trustees, provide an operational perspective on data governance. They oversee efforts to ensure and improve the informational quality, effectiveness, usability, strategic value and security of data. They actively participate in processes that establish data quality as well as definitions and appropriate uses of data elements. They share

in the responsibility to ensure that the Webministry and their respective officers are following this Data Governance Policy.

Data Custodians

Data Custodians are the warranted Webministers of the East Kingdom who use Kingdom data to carry out their jobs. Data Trustees may have additional custodians of data belonging to their Kingdom Offices, which are beyond the scope of this policy. Data Custodians share in the responsibility for managing and protecting data by understanding and following the policies of the East Kingdom Webministry related to data use and data governance. Data custodians have an additional obligation to report data-related problems, updates, and inaccuracies back to the appropriate data steward(s).

Data Access and Use Policies

- Webministers and Kingdom Officers will be granted access to the data needed to do their jobs.
- Access requests will be vetted for compliance with existing Society Policies, Kingdom Law, and applicable Society and Kingdom Officer governing documents.
- Access to data may not be provided by webministers without authorization by an appropriate data trustee.
- Data accessed under the authorization of the relevant data trustee may not be shared without authorization.
- Data Trustees shall be responsible for all data stored centrally on the Kingdom servers and administrative systems, and are responsible for the security of such data.
- Branch and Office webministers, or their Seneschals or Kingdom Officers, are responsible for communicating changes in their group which result in changes to authorized access to data.
- All members of the East Kingdom community are responsible for maintaining the privacy and integrity of all regulated, restricted or confidential data as defined above, and must protect the data from unauthorized use, access, disclosure or alteration.

Data Quality and Security

Data records must be kept up-to-date throughout every stage of the webministry business workflow and in an auditable and traceable manner. Data should only be collected for legitimate uses and to add value to the Kingdom. Extraction, manipulation and reporting of data must be done only to perform Kingdom business, including teaching or research.

Data Retention

Data Trustees will define the standards for the retention of data related to their office, in consultation with the Kingdom Webminister. The East Kingdom Webministry will support data retention standards, and will provide copies of retained data records to Data Trustees upon request. Should Trustees establish a data retention standard that exceeds the policies for the storage of electronic data as defined by the Kingdom Webminister, copies of data records will be provided to the Trustees for storage outside of East Kingdom Webministry maintained systems.

East Kingdom Webministry will retain:

- Websites for each branch, office, guild, and reign while they are active and for at least one year subsequently. Archives will be kept for at least a further two years.
- Email records while an account is active, or until an individual owner deletes it.
- Information submitted for Webministry warranting and reporting while in effect, or for at least 4 years.
- Data added to Webministry maintained systems by Data Trustees or their representatives until requested to be deleted by the appropriate Data Trustee.

Unless otherwise specified, information will be retained until deleted by the individual owner of the data in the case of an individual's own data, or until a written request for deletion is received by the Data Trustee responsible for the data.

East Kingdom Webministry may also transfer data to Data Trustees or their designated Steward or Custodian outside of the Webministry in order to maintain the quality of service offerings to the East Kingdom. Such transfers will be done in consultation with the Data Trustees.