Postgraduate Certificate in Data Governance

Data Security and Data Governance

Data Security is the practice of protecting data from unauthorized access, use, disclosure, disruption, modification, or destruction. It includes a set of policies, technologies, and practices designed to protect data throughout its lifecycle, from creation to disposal. Data Governance, on the other hand, refers to the overall management of the availability, usability, integrity, and security of data. It includes establishing policies, procedures, and standards for data management, ensuring compliance with regulations, and promoting data quality and consistency.

Here are some key terms and vocabulary related to Data Security and Data Governance:

Data Classification

Data classification is the process of categorizing data based on its level of sensitivity, value, and importance. It helps organizations determine the appropriate level of security and access control for different types of data. Common data classifications include public, confidential, and restricted.

Access Control

Access control is the process of granting or denying access to data based on the user's identity, role, and level of clearance. It includes authentication (verifying the user's identity), authorization (determining the user's level of access), and accountability (tracking the user's actions). Examples of access control mechanisms include passwords, biometrics, and two-factor authentication.

Encryption

Encryption is the process of converting plaintext (unencrypted data) into ciphertext (encrypted data) using a mathematical algorithm and a secret key. It helps protect data from unauthorized access, interception, and theft. Examples of encryption algorithms include Advanced Encryption Standard (AES), Triple Data Encryption Algorithm (TDEA), and Rivest-Shamir-Adleman (RSA).

Data Masking

Data masking is the process of concealing sensitive data by replacing it with non-sensitive data while preserving its format and structure. It helps protect data from unauthorized access, exposure, and misuse. Examples of data masking techniques include character substitution, tokenization, and pseudonymization.

Data Backup and Recovery

Data backup and recovery are the processes of creating copies of data and restoring them in case of data loss, corruption, or failure. It helps ensure business continuity, data availability, and data integrity. Examples of data backup and recovery strategies include full backups, incremental backups, differential backups, and disaster recovery plans.

Data Archiving

Data archiving is the process of moving inactive or infrequently used data from primary storage to secondary storage for long-term retention and retrieval. It helps reduce storage costs, improve performance, and ensure compliance with regulations. Examples of data archiving solutions include tape libraries, optical disks, and cloud storage.

Data Quality

Data quality is the degree to which data is accurate, complete, consistent, and timely. It affects the reliability, usability, and value of data for decision-making, analysis, and reporting. Examples of data quality issues include duplicates, inconsistencies, errors, and incompleteness.

Data Lineage

Data lineage is the ability to trace the origin, movement, and transformation of data throughout its lifecycle. It helps ensure data accuracy, completeness, and consistency, and enables data audit, compliance, and governance. Examples of data lineage tools include metadata repositories, data profiling, and data mapping.

Data Privacy

Data privacy is the protection of personal data from unauthorized access, use, disclosure, or destruction. It includes establishing policies, procedures, and standards for data collection, storage, processing, and sharing. Examples of data privacy regulations include General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Health Insurance Portability and Accountability Act (HIPAA).

Data Security Incident

A data security incident is an event that compromises the confidentiality, integrity, or availability of data. It includes unauthorized access, use, disclosure, disruption, modification, or destruction of data. Examples of data security incidents include data breaches, cyber attacks, and insider threats.

Data Security Standard

A data security standard is a set of requirements, guidelines, and best practices for protecting data from unauthorized access, use, disclosure, or destruction. It includes establishing policies, procedures, and technologies for data security, monitoring, and reporting. Examples of data security standards include Payment Card Industry Data Security Standard (PCI DSS), ISO/IEC 27001, and National Institute of Standards and Technology (NIST) Cybersecurity Framework.

In conclusion, Data Security and Data Governance are critical components of data management, ensuring the protection, availability, usability, and integrity of data throughout its lifecycle. Understanding the key terms and vocabulary related to Data Security and Data Governance is essential for data professionals, managers, and executives to make informed decisions, mitigate risks, and comply with regulations. By implementing appropriate Data Security and Data Governance practices, organizations can enhance their

data value, competitiveness, and sustainability.