Task 1

Name	**Major**	**Student ID**
Chen Yinuo	**Digital Technology**	**2023020101**
Fu Yuhan	**Computer Science and Technology**	**2023010218**

Task 2

What is Data? What is Information? What is the difference between Data and Information?

1.Data: Data is a formal representation of facts, concepts, or instructions, which can be in various forms such as numbers, words, images, sounds, etc. For example, a person's height and weight values, a list of employees' names in a company are all data.

2.Information: Information is data that has been processed, organized, and interpreted and has meaning and value for the receiver. For example, by analyzing the height data of students in a class and obtaining the average height and height distribution, etc., these conclusions are information.

3.Difference: Data is the raw material, the unprocessed facts; while information is obtained by processing and analyzing data and can provide a basis for decision-making and action.

What is Metadata? Why we need metadata?

1. **Metadata**: Metadata is data about data, which describes the characteristics, source, structure, quality, etc. of data. For example, the field names, data types, lengths, etc. of a database table are the metadata of the table data; the shooting time, resolution, shooting equipment, etc. of a picture are also metadata.

2. **Why we need it**:

A.To help understand data: Metadata provides the background and context information of data, enabling users to better understand the meaning and use of data.

B.For data management: It helps in the organization, storage, retrieval, and maintenance of data. For example, in a database, metadata can quickly locate the required data.

C.For data sharing and exchange: When different systems share and exchange data, metadata can ensure the consistency and accuracy of data, enabling the receiver to correctly use the data.

Task 3

What is Data Privacy?

1.Data privacy refers to the protection of data by individuals or organizations to ensure that data is not accessed, used, disclosed, or modified without authorization. It involves protecting sensitive data

such as personal identity information, financial information, health information, etc.

Some key elements (practices, rules, guidelines, tools) that organizations use to maintain data privacy compliance

1.Practices:

A.Data classification and grading: Classify data and manage it according to its sensitivity level, taking different protection measures for different levels of data.

B.Access control: Establish a strict access control mechanism so that only authorized personnel can access relevant data.

C.Employee training: Train employees on data privacy to raise their privacy awareness and ensure that they comply with data privacy regulations in their daily work.

2.Rules and guidelines:

A.Laws and regulations: Comply with relevant national and local laws and regulations, such as the "Cyber Security Law of the People's Republic of China" and the "Data Security Law of the People's Republic of China", which have clear requirements for the protection of data privacy.

B.Industry standards: Follow the privacy standards and guidelines of the industry, such as HIPAA (Health Insurance Portability and Accountability Act) in the medical industry.

3.Tools:

A.Encryption technology: Use encryption algorithms to encrypt data so that data exists in ciphertext form during transmission and storage, and only those with the correct key can decrypt the data.

B.Data desensitization tools: Desensitize sensitive data, hiding the sensitive parts of data without affecting its use value.

The importance of data privacy for individuals and businesses and the differences between them

1.For individuals:

A.Protecting personal rights and interests: Personal privacy data contains a large amount of sensitive information such as ID numbers and bank card numbers. If leaked, it may lead to personal property losses and identity theft. Protecting data privacy can safeguard personal legal rights and interests.

B.Maintaining personal dignity: Some personal privacy information such as health status and religious beliefs, if improperly disclosed, may harm personal dignity.

2.For businesses:

A.Maintaining business reputation: If a business has a data leak event, it may damage its reputation, leading to customer loss and affecting its economic benefits.

B.Complying with laws and regulations: Businesses must comply with relevant laws and regulations, and maintaining data privacy is a necessary condition for legal business operation.

3.Differences:

A.Different focuses: Individuals focus more on the protection of personal identity information and life privacy; businesses focus more on the protection of business secrets and customer information.

B.Different impact ranges: The leakage of personal data privacy mainly affects the individual; the leakage of business data privacy may affect a large number of customers and have a wide impact on the business operation and social image.

Task 4

What is Database Security?

Database security refers to ensuring the security of a database system through a series of tools, processes, and methods, including protecting the data stored in the database as well as the database management system itself. It aims to prevent the database from being

attacked by malicious cyber-attacks, software vulnerabilities, invasion, misuse or carelessness, and damage.

Some methods and measures for database security

1.Tools:

A.Firewall: Set up a firewall between the database server and the external network to prevent unauthorized external access.

B.Intrusion Detection System (IDS) and Intrusion Prevention System (IPS): Detect and prevent the database system from being invaded. IDS can detect abnormal behavior and issue an alarm, and IPS can take measures to prevent the invasion when detecting the invasion.

C.Encryption tools: Encrypt sensitive data in the database, such as using symmetric encryption algorithms (such as AES) or non-symmetric encryption algorithms (如 RSA).

2.Processes and methods:

A.Authentication and authorization: Establish a strict authentication and authorization mechanism to ensure that only authorized users can access the database. Users need to provide correct usernames and passwords and other credentials, and different access levels are assigned according to the user's role and permissions.

B.Data backup and recovery: Regularly backup the database so that data can be quickly recovered in case of data loss or damage. The

backup frequency and strategy should be determined according to the importance of the data and its change frequency.

C.Security audit: Audit the access and operation of the database, record the access time, operation content, etc. of users, so that the responsibility can be traced in case of a security problem.