Data Security, Ethical and Compliance Considerations

As a database administrator (DBA), one of the most important parts of your role is to safeguard the data in the system. You control the system, so you are responsible for ensuring that the data is secure and complies to all relevant standards. You must also hold yourself to the highest ethical standards. Some organizations include a specific database security administrator role that focuses on these duties, but all DBAs need to keep them in mind.

::page{title="Fundamental Ethics"}

A foundation of basic ethical concepts supports good data security practices. These should help guide the policies and workflows you create and the actions you take. Some important concepts are:

- **Transparency**: When you collect information, you should tell the owners of the information exactly what data you will collect and what you will do with it. Inform them about how you use the data, how you store it, who will have access to it, and how you will dispose of it when you have finished using it.
- **Consent**: You should get clear consent from data owners before you collect their data. This should detail what data you will be allowed to collect and how you will be allowed to use it.
- **Integrity**: Always be clear about your procedures and policies, and always follow them consistently. As far as you can, make sure that others in your organization also follow the correct procedures and policies.

Consider creating a code of ethics–a written statement of security-related standards and intentions. You can include priorities, best practices, who will be responsible, and whatever else is important to understand clearly. This will create shared expectations for yourself and others, which will help build trust and make it easier for everyone to follow correct procedures.

Secure System Design

The structure of your system is a powerful tool in keeping your data safe. If your system is built to maintain security, it's much easier to prevent breaches. To make sure your system works for you, consider these factors.

- **Protection from malicious access**: The front line of protection for your data is basic software security. Your firewall and other cybersecurity tools should actively prevent hacking and malware installation, and alert you to threats. Be sure you update this software frequently, to keep scanning lists up to date. Also, educate users about phishing and other ways that they can unwittingly enable malicious access.
- **Secure storage**: The storage you choose for your data must be secure not only from malicious access, but also from hardware failure and even natural disasters. Select your services carefully and make sure you understand their security practices and disaster preparedness plans. Back up your data regularly and reliably to minimize data loss in case of an emergency.
- **Accurate access**: Only those who need certain data should be able to access it. Establish a system of assigning and tracking privileges that assigns each user only the necessary privileges, and controls what they can do with the data. Ensure that your policy complies with any data usage agreements you have made.
- **Secure movement**: Data can be particularly vulnerable to interception when you move it into or out of storage. Be sure to consider safe transfer methods as carefully as you plan safety for the rest of your system.
- **Secure archiving**: At some point, you may want to move data from active storage to an archive. This can protect it from accidental access and make your system more efficient. Make sure your archiving system is as secure as the rest of your storage. Data agreements often specify how long you may use the data, so be sure the archived data is regularly weeded for expired rights and don't retain any more data than you will need for compliance with organization policy. Eliminate your discarded data securely and completely.

Compliance Issues

Maintaining compliance with all relevant laws and standards is a vital concern. Failure can result in data insecurity, professional censure for your organization, and even legal action. This list includes some of the most common types of standards, but it's not exhaustive; always find out which regulations and standards apply to your organization.

- **National/international regulations**: Many industries must be concerned with important legal standards on the national or international level. Some examples include HIPAA regulations for health-related information in the US, the GDPR in Europe, and the Information Technology Act, 2000 in India.
- **Industry standards**: Some data standards aren't enforced by law but can still carry repercussions for your organization's reputation and standing if they aren't followed. An example might be the Payment Card Industry Data Security Standard (PCI DSS), which applies to any organization that collects, stores, or transmits cardholder data.
- **Organization best practices**: Each organization will formulate standards for handling its internal data; as a DBA, you may work on that as part of your job. Employee confidentiality is often an important part of these policies, as is protecting intellectual property owned by the organization.

If you build your system and procedures thoughtfully and maintain them with consistency and vigilance, you can keep the data in your system safe and productive.