

# Read More About Snowflake Security and Compliance

---

 [coursera.org/learn/snowflake-snowpro-core-certification-preparation/supplement/DSIdC/read-more-about-snowflake-security-and-compliance](https://coursera.org/learn/snowflake-snowpro-core-certification-preparation/supplement/DSIdC/read-more-about-snowflake-security-and-compliance)

## 1. Snowflake Security Features Overview:

- Snowflake offers robust security capabilities including network security, access control, and authentication.
- Features like automatic encryption of data at rest and in transit, ensuring data is always protected.
- Provides fine-grained access controls and role-based access management to regulate who can access what data and how.

[Read More](#)

## Implementing Data Encryption and Masking:

- Snowflake automatically encrypts all data stored in its platform, using strong encryption standards.
- For additional security, Snowflake also supports dynamic data masking. This allows sensitive data to be masked or obscured based on user roles and privileges, ensuring that only authorized personnel can view sensitive information.

[Read More](#)

## Compliance and Governance in Snowflake:

- Snowflake complies with major global and industry-specific regulations like GDPR, HIPAA, PCI DSS, and more, ensuring that data management practices meet required legal standards.
- Offers features for data governance, including data lineage, auditing capabilities, and detailed access logs, which help in tracking and monitoring data access and modifications, crucial for regulatory compliance.

[Read More](#)

---

Let me know if you have any questions about this material. I'm here to help!