**Database Security**

**Security Management:**

* Password Policies
  + 3 Month Password Expiration
    - No repeat passwords
  + Password Criteria
    - Minimum Length 12 Characters
    - Must include at least one number
    - Must include Special Character
  + Two-Factor Authentication on login
    - Can be turned off for periods of 2 weeks at a time
  + Possible use of password managements system
* Employment Policies
  + Centralized Access Management
    - Centralizing logins enables easy monitoring of access permissions, facilitates quick updates, and provides a single point of control for modifying or revoking access as needed.
  + Role Based Access Control
    - Create roles based on employees needs
      * For example a custodian would not need any permissions except possibly access through key card to a hardware closet
      * Role-based permissions are reviewed periodically to confirm that each employee's access aligns with their current responsibilities.
      * Minimizes risk of unnecessary access to important data
    - Onboarding
      * No generic or shared accounts are allowed
      * New employees should be trained in best practices for database security
      * Training on phishing attacks and password management
    - Offboarding
      * When an employee leaves the organization, their access must be promptly removed
      * Revoke Logins from all systems
      * Update passwords for administrative accounts if necessary
    - All logins should be stored and logged along with changes made to accounts
    - Access Review and Verification
      * Periodic access reviews are essential to ensure compliance with these policies
      * Regular reviews of login records and permissions
* Remote Access
  + Multi-Factor Authentication required on all remote access logins
  + Call-back system if login fails
  + Approval of IP ranges
  + Access Control of who can use remote access
  + Auditing of remote logins
* Vendor Access
  + Network Segmentation and Dual-Firewall Structure
    - Vendor Access is restricted to a segmented network
    - Network is in between two firewalls
  + Role Based Access Control
    - Vendors should be granted the minimum level of access necessary to perform their functions
  + Periodic Access Auditing and Monitoring
* Non-Employee Access
  + All customers or external users must complete a registration process to establish their identity before gaining access to their accounts
  + Secure Server and Network Design
    - Customer access should be managed through dedicated, secure servers separate from internal network servers
    - These servers should be hosted within a protected network segment and employ strong encryption protocols (such as HTTPS/TLS) to secure all data exchanges
  + MFA on login
  + Continuous Monitoring and Intrusion Detection
    - Customer access points should be continuously monitored using automated tools to detect unusual activity or potential intrusions.
  + User Education and Security Awareness
    - Customers should be provided with resources on securing their accounts, including tips on creating strong passwords, recognizing phishing attacks, and understanding multi-factor authentication

**Physical Security:**

* Access Control Systems
  + Secure areas, such as data centers and rooms with sensitive information, must be protected using card access systems or biometric verification methods
  + Access should be granted based on role requirements and reviewed periodically
* Multi-Layered Access Zones
  + Public Zones: Areas accessible to visitors and general employees
  + Restricted Zones: Areas like server rooms, which require additional access credentials
  + High-Security Zone**s**: Areas with sensitive data or equipment, accessible only to essential personnel with enhanced access controls
* Surveillance and Monitoring
  + Surveillance cameras should be strategically placed throughout secure areas to monitor access and activities
  + Cameras should cover all entry points, restricted zones, and high-security zones
  + Monitoring should be continuous, with security personnel alerted to unusual activity
* Security Personnel and Guard Patrols
  + Security guards should be stationed at key entry points and conduct regular patrols within restricted and high-security zones
* Intrusion Detection Systems
  + Sensitive areas should be equipped with intrusion detection systems (i.e., motion sensors or alarms)
* Visitor Access Protocols
  + All visitors must sign in at the front desk, provide valid identification, and wear visitor badges while on-site
* Regular Security Assessments and Drills
  + Regular physical security assessments should be conducted to evaluate the effectiveness of access controls, surveillance, and intrusion detection systems
* Equipment and Asset Security
  + All sensitive equipment and portable assets should be securely stored in locked rooms or cabinets when not in use
  + Access to high-value or sensitive assets should be limited to authorized personnel only, and usage logs should be maintained
* Policy Compliance and Audit
  + Physical security policies and access logs should be reviewed and audited regularly to identify compliance gaps and security weaknesses

**Network Security**

* Principle of Least Privilege
  + Network permissions should adhere to the principle of least privilege, granting users and administrators only the access necessary to perform their roles
* Separation of Database and Network Administrator Roles
  + Separate roles should be created for database and network administrators, ensuring that each group has only the access needed to perform their specific responsibilities
* MFA
* Network Segmentation and Firewalls
  + Database servers should reside on a separate, segmented network protected by firewalls that restrict access to only authorized IP addresses and devices
  + Firewalls should be configured to block all unnecessary traffic to and from the database servers, minimizing the risk of unauthorized access
* Security Patch Management
  + All network components, including database servers, should be kept current with security patches
* Incident Response and Remediation
  + In the event of a network security breach that may affect database security, the incident response team should follow a predefined protocol to contain and investigate the breach
  + This includes securing affected accounts, reviewing access logs, and addressing any network misconfigurations

**Database Security:**

* Server-Level Security
  + Server Roles**:** Only necessary personnel should be assigned powerful server roles
    - Administrator/Manager: Has unrestricted access across all databases on the server and should be assigned only to essential personnel
    - Security Officer: Has the ability to create and manage logins but does not have direct access to database content
    - Database Creator: Can create new databases on the server but does not inherently have full access to existing databases
* Database-Level Security
  + Object-Level Permissions: Within a database, permissions should be assigned at the object level (e.g., tables, views, stored procedures). This allows fine-tuned access control based on user needs without exposing unnecessary data
  + User Access Review and Role Audits: Regular audits should be conducted to review users’ database-level permissions, ensuring that access aligns with current responsibilities and is revoked when no longer needed
* Stored Procedures for Data Access
  + Controlled Access**:** Stored procedures should be used for all database interactions involving sensitive data, ensuring users cannot access or modify data directly
  + Permissions Management: Access to stored procedures should be granted only to users who require it, helping to enforce application-specific permissions and data integrity
* Views for Data Security and Access Control
  + Data Masking and Filtering: Views should be used to filter and mask sensitive data (I.E., hiding Social Security numbers) where only partial data is necessary for user functions
  + Layered Security with Views: Combining views with stored procedures creates a layered security model, where users can retrieve and interact with data in controlled ways without direct table access.
* Embedded SQL and Application Security Policy
  + Avoid Hardcoding Credentials: Application-level SQL code should never contain hardcoded credentials. All credentials should be securely managed through the database server or an external authentication system
  + Parameterized Queries to Prevent SQL Injection: SQL statements should use parameterized queries to prevent SQL injection attacks. Dynamic SQL should be avoided unless absolutely necessary, as it increases the risk of SQL injection vulnerabilities.
* Logging and Auditing of Access and Actions
  + Review Frequency: Logs should be reviewed on a regular schedule, with automated alerts configured for suspicious or unauthorized access attempts
  + Data Retention Policy**:** Logs should be retained according to the organization’s data retention policies and archived securely for future auditing needs