DB Info (Data)	Top Management	HR	IT/ Sec	Sales & Mark	Fin & Accont	Operation
Financial info	CO (+), CPO (Read Only), CTO (Read Only)				(+)	-
Staff Info	CO (+), CPO (Read Only),CTO (Read Only)	(+)	(+)		(+)	(+)
Customer Info	CO (+), CPO (+), CTO (+)			(+)		(+)
IT Sector	CO (read only), CPO (read only), CTO (+)		(+)			(+)
Sec & Monitoring	CO (Read Only),CPO (Read Only),CTO (Read Only)		(+)			(+)
Sales & Marketing	CO (+),CPO (+),CTO (Read Only)			(+)		

All Team leads can open ticket to Operation team and ask Temporary DB access

1. **Just-in-Time (JIT) access:** This is a security model where users are granted privileged access to a database only when they request it and for a limited duration.
2. **Temporary tables:** This refers to creating tables that only exist for the duration of a user's current database session.

Temporary DB Access & Security Policy Confirmation

Your points cover strong measures across three main areas: User Access, Data Protection, and Monitoring.

1. User & Device Security (PC/Laptop & General Staff)

Security Requirement	Details	Security Principle
Login Passwords	All staff (PC or laptop login pass) must use a Strong Pass.	Authentication
Password Updates	PC/Laptop passwords must be updated every 3 months.	Password Hygiene

Multi-Factor Authentication (MFA)	Daily MFA for PC/Laptop login is required for ALL staff.	Strong Authentication

2. Database (DB) Access Security

Security Requirement	Details	Security Principle
DB Login	Must use a Strong Pass.	Authentication
Two-Factor Authentication (2FA)	2FA by session is required. The clarification is excellent: if a user is passive (i.e., not actively using the DB for a set period), they must pass the 2FA step upon re-access.	Zero Trust / Continuous Authentication

3. Email Security

Security Requirement	Details	Security Principle
Password Strength	Strong pass required; must be updated every 3 months.	Password Hygiene
Multi-Factor Authentication (MFA)	MFA for email login is required.	Strong Authentication
SMS MFA	SMS MFA specifically in the login step adds a layer of possession-based security.	Strong Authentication
Logout Frequency	Logout every week is required to enforce re-authentication and session freshness.	Session Management

4. Data Protection and Monitoring

Security Requirement	Details	Security Principle
BackUP Data	BackUP Data must be encrypted using AES (a strong industry standard).	Data at Rest Encryption
Monitoring	Database logs must be dedicated to a Firewall log. This suggests central logging for security analysis.	Auditing & Visibility

Notification	Email and SMS notification to the SEC-DEV team for suspicious or critical events. The repeated SMS notification to SEC-DEV team emphasizes high-priority alerting.	Incident Response & Alerting

5. Wi-Fi Network Access Security (Dual Network Policy)

Component	**Authentication/Encryption**	**Access Policy**	**Key Security Measures**
Explanation & Security Value	**WPA3-Enterprise** (Required) with **802.1X** via central **RADIUS server**. This provides **strongest modern encryption** and **centralized user authentication**. The RADIUS server acts as the single point of truth for validating user credentials against a directory (like Active Directory) before granting network access.	**Multi-Factor Authentication (MFA)** is mandatory. This is a critical control that ensures access requires **two or more verification factors** (e.g., password + one-time code), dramatically reducing the risk of unauthorized access due to compromised credentials.	**Network Isolation (VLANs):** Creates virtual, logical separation of the staff network from all others. **Client Isolation:** A crucial defense-in-depth measure that prevents connected staff devices from directly interacting with each other, limiting the spread of malware or the ability of an attacker to "see" other devices on the network.

Guest Wi-Fi (Controlled Access)

Component	**Authentication/Encryption**	**Access Policy**	**Key Security Measures**

Explanation & Security Value	**WPA2/WPA3-Personal** (Passphrase-based). Provides standard encryption for a publicly accessible service.	**Monthly Passphrase Updates** and **Time-Limited Access** (e.g., auto-disconnect after 8 hours) are standard practices to limit the lifetime of credentials and ensure resource availability.	**Captive Portal:** Forces users to agree to **Terms of Use** (ToU) before connecting. This is vital for **legal liability** purposes and often includes logging user device MAC addresses. **Content Filtering:** Blocks access to high-risk (e.g., known malware distribution) or high-bandwidth (e.g., illegal streaming) sites, protecting network resources and mitigating legal risks.

6. Advanced Monitoring & Incident Response

This section defines the technical and procedural requirements for **proactive security operations** to ensure the **confidentiality, integrity, and availability** of network and data assets.

Security Requirement	Details/Implementation	Security Principle Applied
Intrusion Detection/Prevention	Deployment of a **Wireless Intrusion Detection System (WIDS)**. This system actively scans the RF environment to **detect and alert on rogue Access Points (APs)** and unauthorized wireless devices trying to mimic the internal network or conduct denial-of-service attacks.	Detection & Prevention
Centralized Logging	**Aggregation of all security-relevant logs** (Wi-Fi, database access, failed logins) into a single platform (e.g., a **SIEM**) for **real-time monitoring** by the **SEC-DEV team** (Security & Development/Operations). This enables rapid correlation of events across systems for faster incident response.	Auditing & Accountability
System Patching	**Monthly patch cycles** for all critical network infrastructure components (APs, routers) and servers. This is the primary control for **eliminating known software vulnerabilities** that could be exploited by attackers.	Vulnerability Management