### **Data leak worksheet**

| **Aspect** | **Description** |
| --- | --- |
| Incident Summary | Sales manager accidentally shared sensitive data, leading to a data leak. Lack of clear access controls and reminders for the sales team |
| Control (Least Privilege) | Company lacks proper access control and least privilege principles. |
| Review (NIST SP 800-53: AC-6) | NIST SP 800-53: AC-6 focuses on least privilege and access control. "Least Privilege" principle emphasizes minimal access for users. |
| Recommendations | Improvements to implement least privilege: |
|  | - Role-Based Access Control (RBAC) |
|  | - Automated Access Revocation |
|  | - Access Activity Logging |
|  | - Regular Privilege Audits --------  1. User Education and Reminders 2. Access Request and Approval Workflow |
| Justification (Addressing Issues) | - RBAC restricts unauthorized access |
|  | - Automated access revocation prevents lingering permissions |
|  | - Access activity logs aid in monitoring and incident response |
|  | - Regular audits ensure proper access alignment and reduce  risks  Justification for Recommendations  - User Education reduces the risk of accidental data sharing. Approval Workflow ensures access aligns with business needs. |