Data leak worksheet

Incident summary: A sales manager shared access to a folder of internal-only documents with their team during a meeting. The folder contained files associated with a new product that has not been publicly announced. It also included customer analytics and promotional materials. After the meeting, the manager did not revoke access to the internal folder, but warned the team to wait for approval before sharing the promotional materials with others.

During a video call with a business partner, a member of the sales team forgot the warning from their manager. The sales representative intended to share a link to the promotional materials so that the business partner could circulate the materials to their customers. However, the sales representative accidentally shared a link to the internal folder instead. Later, the business partner posted the link on their company's social media page assuming that it was the promotional materials.

Control	**Least privilege**
Issue(s)	*What factors contributed to the information leak?* Violation of the Principle of Least Privilege Issue: Employees had access beyond what was needed for their roles. NIST Reference: AC-6 (Core) — “Employ the principle of least privilege, allowing only authorized accesses necessary to accomplish assigned tasks.” Lack of Role-Based Access Controls (RBAC) Issue: Absence of clearly defined roles and separation of duties. NIST References: AC-6 (2) — “Require users with access to security functions to use non-privileged accounts when accessing nonsecurity functions.” AC-3 – Access Enforcement (Related Control) — Supports RBAC by enforcing access authorizations. Inadequate Data Sharing Restrictions

	Issue: System permitted unrestricted external sharing of sensitive data. NIST References: AC-6 (8) — “Prohibit privileged access to the system by non-organizational users.” PL-4 – Rules of Behavior (Related Control) — Defines acceptable data sharing and user responsibilities. Human Error & Lack of Awareness Issue: Accidental sharing due to lack of user awareness or training. NIST References: AT-2 – Security Awareness Training (Cross-Control) — “Provide training to all users to recognize and respond to security risks.” No Regular Privilege Review Issue: Privileges were not periodically reviewed or adjusted. NIST Reference: AC-6 (9) — “Review privileges assigned to users to validate need; reassign or remove if necessary.”
Review	*What does NIST SP 800-53: AC-6 address?* NIST SP 800-53: AC-6 addresses the principle of least privilege, requiring that users and processes are granted only the minimum access necessary to perform their assigned tasks, helping to reduce the risk of unauthorized access and data breaches.
Recommendation(s)	*How might the principle of least privilege be improved at the company?* Implement Role-Based Access Controls (RBAC) Action: Define and enforce roles that grant only the minimum necessary permissions for each job function (e.g., sales, support, development). NIST References: AC-6 (Core) – Enforces least privilege per task. AC-6 (2) – Non-Privileged Access for Nonsecurity Functions: Supports RBAC models to prevent misuse of privilege. AC-3 (Related Control) – Access Enforcement: Ensures roles only allow access as authorized.

	Conduct Regular Privilege Reviews Action: Review all user privileges at defined intervals to ensure they still align with business needs and revoke unnecessary permissions. NIST Reference:

	AC-6 (7) – Review of User Privileges: Requires periodic validation and correction of privilege assignments. Enforce Separation of Duties & Processing Domains Action: Use technical solutions like virtual machines, VLANs, or domain separation to minimize cross-access between roles. NIST References: AC-6 (4) – Separate Processing Domains: Enables finer-grained privilege enforcement using logical or physical separation. Restrict Privileged Access to Authorized Organizational Users Action: Ensure only trusted employees or vetted contractors are granted elevated access rights. NIST Reference: AC-6 (6) – Privileged Access by Non-Organizational Users: Prohibits elevated access by untrusted or external users. Implement a Privileged Access Management (PAM) System Action: Use PAM tools to control, monitor, and log the use of all privileged accounts. NIST References: AC-6 (1) – Authorize Access to Security Functions: Control access to critical security functions and data. AC-6 (9) – Log Use of Privileged Functions: Audit all uses of elevated privileges for accountability. Provide Targeted Training on Least Privilege Principles Action: Educate staff on proper data handling and access protocols through mandatory awareness training.

	NIST Reference: AT-2 (Related Control) – Security Awareness Training: Ensures users understand the importance of limited access. Enforce Use of Non-Privileged Accounts for Routine Tasks Action: Require privileged users (e.g., admins) to use standard accounts for day-to-day operations unless elevated access is explicitly needed. NIST Reference:

	NIST Reference: AC-6 (2) – Non-Privileged Access for Nonsecurity Functions
Justification	*How might these improvements address the issues?* 1. Implement Granular Role-Based Access Controls (RBAC) What to Do: Define precise roles (e.g., sales rep, sales manager, marketing, dev) and restrict access to internal-only contentbased on job necessity. How It Helps: Prevents all sales team members from accessing high-risk internal documents unless explicitly needed. NIST Reference: AC-6 (Core) – Principle of Least Privilege AC-6 (2) – Non-Privileged Access for Nonsecurity Functions AC-3 – Access Enforcement 2. Use Time-Bound and Purpose-Limited Access What to Do: Apply automatic expiration or review-based access after meetings or projects. How It Helps: If access to the folder had been automatically revoked after the meeting, the accidental sharing would not have occurred. NIST Reference: AC-6 (7) – Review of User Privileges CM-5 – Access Restrictions for Change 3. Restrict External Sharing Capabilities by Default

	What to Do: Disable link sharing or limit sharing to internal users unless explicitly approved. How It Helps: Prevents external parties from accessing internal folders unless someone deliberately overrides a sharing policy. NIST Reference: AC-6 (6) – Privileged Access by Non-Organizational Users PL-4 – Rules of Behavior SC-12 / SC-13 – Cryptographic Protection of Data in Transit (if using access-controlled links) 4. Implement Data Loss Prevention (DLP) Policies

	What to Do: Use DLP solutions to detect and block sharing of sensitive documents or internal links through email or chat. How It Helps: Stops the accidental transmission of confidential content like the folder link. NIST Reference: AC-6 (10) – Prohibit Non-Privileged Users from Executing Privileged Functions SI-4 – System Monitoring 5. Log and Monitor Privileged Actions What to Do: Enable logging for actions such as link sharing, folder access changes, and file downloads. How It Helps: Improves auditability, detects policy violations, and provides early warning of leaks. NIST Reference: AC-6 (9) – Log Use of Privileged Functions AU-2 / AU-12 – Audit Events / Audit Data Analysis 6. Provide Training Focused on Access Risks & Link Sharing What to Do: Conduct awareness training specifically on secure data sharing, access hygiene, and link management. How It Helps: Reduces human error — like forgetting to check what link is being
	shared. NIST Reference: AT-2 – Security Awareness Training