

Incident handler's journal

Date: 12/04/2023	Entry: 001
Description	Internal-only product files were inadvertently shared with external parties due to insufficient access restrictions and user error during a partner video call.
Tool(s) used	
The 5 W's	<p>Who caused the incident? A sales representative (name withheld) accidentally shared a link to an internal folder during a partner video call.</p> <p>What happened? The internal folder—containing unreleased product details, customer analytics, and promotional material—was shared externally. A partner then posted the link on their social media</p> <p>When did the incident occur? During a business partner video meeting shortly after a team meeting where folder access had been granted.</p> <p>Where did the incident happen? Virtually, via a cloud-based file-sharing platform during a video conference call.</p> <p>Why did the incident happen? Violation of the Principle of Least Privilege—employees had access to more data than needed.</p> <p>No Role-Based Access Control (RBAC) was enforced.</p> <p>No automated expiration or restrictions for temporary access.</p> <p>Lack of training led to accidental link sharing.</p> <p>No external sharing restrictions in place.</p>
Additional notes	<p>NIST SP 800-53 AC-6 (Least Privilege) and AT-2 (Security Awareness Training) directly relate to the root causes.</p> <p>Recommendations include implementing RBAC, restricting external sharing by default, deploying a PAM solution, and improving awareness training focused on access hygiene.</p>