SOP
Access Control Incident & NIST Alignment

v1.2.1

Author:
Eldon Gabriel

March 20, 2025

Security Systems Specialist

Table of Contents

Revision History

Version	Date	Author	Description of Changes
1.0.0	02/12/2025	Eldon G.	Initial draft.
1.0.1	02/22/2025	Eldon G.	Added cover, table of contents, and revision history.
1.2.0	07/09/2025	Eldon G.	Added sectioning, numbering, and conclusion.
1.2.1	03/20/2026	Eldon G.	Aligned incident analysis with NIST 800-53 (AC-6); added an executive summary and mapped technical failures to organizational risk mitigation strategies.

0.0 Executive Summary

0.1 Project Overview

Access Control Incident Analysis & NIST Alignment

This report explains how a data exposure incident occurred owing to weak access control settings. Failure in access restrictions allowed internal design materials to be shared outside the organization.

This project sought to identify the root cause of the issue and understand what went wrong. The analysis considers both technical failures and poor policy enforcement. It also maps the problem to the **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 framework** to guide the appropriate fixes.

Project Objective

The main goal was to investigate how sensitive the files were to loose sharing settings. The system relied too much on trust instead of proper security controls.

This project focuses on replacing trust-based access with enforced security rules. It follows the **Principle of Least Privilege (POLP)**, which dictates that users should have access only to the resources they require and nothing more.

Technical Analysis & Control Mapping

The incident was reviewed using standard security frameworks to understand failures and plans for improvements.

Incident Analysis: Compared the expected access (who should have access) with the actual access (who actually had access). This revealed that the permissions were too open.

NIST SP 800-53 Alignment: The issue maps to **AC-6 (Least Privilege)**. The organization did not properly limit user access or enforce role-based controls.

NIST Cybersecurity Framework (CSF): The response aligns with

- **Protect (PR.AC):** Improve access control and identity management
- **Detect (DE.CM):** Monitor systems to detect misuse or abnormal access

Risk Mitigation Plan: A security plan was created with the following components:

- Automatic expiration of shared links
- Domain restrictions (only approved domains allowed)
- Regular access reviews

Validation & Recommendations

To prevent this from occurring again, the following actions are recommended:

Technical Enforcement: Replace manual sharing with system-enforced rules, such as setting default access to “**Internal Only**.”

Audit Process: Run regular access reviews to remove unnecessary permissions and stop “permission creep.”

User Awareness: Provide role-based training to users on the appropriate handling of sensitive data.

1.0 Access Control Incident Report

1.1 Project Description

This report examines an incident in which sensitive internal files were disclosed by mistake due to poor access controls. The goal was to determine what went wrong, identify the relevant control failures, and propose improvements that meet the NIST standards to prevent similar incidents in the future.

1.2 Incident Overview

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 had 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 a warning from their manager. The sales representative intended to share a link to promotional materials so that the business partner could circulate the materials to their customers.

However, the sales representative inadvertently shared a link to the internal folder instead. Subsequently, the business partner posted the link on their company's social media page, assuming that it contained promotional materials.

Impact

Exposure of more than 15 sensitive design documents to unauthorized external domains.

1.3 Control Analysis

Control	Least Privilege
Issue(s)	*Internal folder access was not restricted to the manager and the sales team. The business partner should not have received or had permission to share promotional information on social media.*
Review	*NIST SP 800-53: AC-6 emphasizes POLP, ensuring that users have only the minimal access required to perform their tasks. It also recommends control enhancements to strengthen data privacy and improve access management.*
Recommendation(s)	• *Restrict access to sensitive resources based on user roles.* • *Regularly audited user privileges.*
Justification	*Data leaks can be prevented by restricting shared links to internal files for employees. Additionally, requiring managers and security teams to conduct regular audits of team file access would help limit exposure to sensitive information and ensure that only authorized individuals have access.*

2.0 Security Plan Snapshot

2.1 NIST CSF Mapping

Function	Category	Subcategory	Reference(s)
Protect	PR.DS: *Data security*	PR.DS-5: *Protection against data leaks.*	*NIST SP 800-53: AC-6*

This incident falls under the **Protect** function of the NIST CSF, specifically addressing **data security (PR.DS-5)**. The relevant control from NIST SP 800-53 is **AC-6: Least Privilege**.

2.2 NIST SP 800-53: AC-6 – Least Privilege

NIST developed SP 800-53 to provide businesses with a customizable information privacy plan. It is a comprehensive resource that describes a wide range of control categories. Each control provides a few key pieces of information:

- **Control:** What is the requirement?
- **Discussion:** The importance of the control and how it should be applied.
- **Control enhancements:** Additional recommendations to improve effectiveness.

The control **AC-6 (Least Privilege)** is the sixth in the Access Control (AC) family and is a cornerstone for minimizing unauthorized access.

2.3 AC-6 Control Details

AC-6	**Least Privilege**
	Control: *Access should be minimal, and task completion requires authorization.*
	Discussion: *Implement processes, user roles, and privileges as necessary to achieve the principle of least privilege. The aim is to prevent over-permissioned access, which could lead to unintended exposure or misuse of information.*
	Control Enhancements: ● *Access to sensitive files based on roles* ● *Automatic expiration of access rights* ● *Logging and reviewing account activity.* ● *Periodic privilege audits*

Note: *In the Access Control family of NIST SP 800-53, Least Privilege is listed as the sixth control (AC-6). This highlights its foundational importance in securing information systems and enforcing responsible data access.*

3.0 Conclusion

3.1 Key Takeaways

- Access controls must be enforced beyond verbal communication; policies must be enforced via technology.
- Least privilege is not a one-time configuration, but a continuous practice.
- Public exposure to internal resources often stems from permission mismanagement, not malice.

3.2 Security Implications and Recommendations

Reinforce Technical Safeguards: Implementing automated link expiration, defaulting to internal-only sharing, and restricting external domains.

Standardize File Access Reviews: Weekly or bi-weekly audits should be scheduled, particularly for files linked to product development or customer data.

Train Staff Continuously: Conduct quarterly training on secure file sharing and incident reporting protocols.