REPORT Access Control Incident

v1.2.0

Author:

Eldon Gabriel

July 9, 2025

TABLE OF CONTENTS

TABLE OF CONTENTS 1
REVISION HISTORY 2
SECTION 1.0: ACCESS CONTROL INCIDENT REPORT 3
1.1 Project Description 3
1.2 Incident Overview 3
1.3 Control Analysis 4
SECTION 2.0: SECURITY PLAN SNAPSHOT 5
2.1 NIST Cybersecurity Framework Mapping 5
2.2 NIST SP 800-53: AC-6 – Least Privilege 5
AC-6 Control Details 6
SECTION 3.0: CONCLUSION 7
3.1 Key Takeaways: 7
3.2 Security Implications and Recommendations: 7

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	02/12/2025	Eldon G.	Initial draft.
v1.0.1	02/22/2025	Eldon G.	Added cover, table of contents, and revision history.
v1.2.0	07/09/2025	Eldon G.	Added sectioning, numbering, and conclusion.

SECTION 1.0: ACCESS CONTROL INCIDENT REPORT

1.1 Project Description

This report looks at an incident where sensitive internal files were disclosed by mistake due to poor access controls. The goal is to find out what went wrong, identify the relevant control failures, and propose improvements that meet NIST standards to stop something like this from happening again.

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 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 promotional materials.

1.3 Control Analysis

Control	**Least Privilege**
Issue(s)	*The internal folder access was not restricted to the manager and the sales team. The business partner shouldn't have received or had permission to share the promotional information to social media.*
Review	*NIST SP 800-53: AC-6 emphasizes the Principle of Least Privilege, ensuring users only have 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 role. ● Regularly audit user privileges.
Justification	*Data leaks can be prevented by restricting shared links to internal files to employees only. 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.*

SECTION 2.0: SECURITY PLAN SNAPSHOT

2.1 NIST Cybersecurity Framework Mapping

Function	Category	Subcategory	Reference(s)
Protect	PR.DS: *Data security*	PR.DS-5: *Protections 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's a comprehensive resource that describes a wide range of control categories. Each control provides a few key pieces of information:

- **Control:** What the requirement is.
- **Discussion:** Why the control matters and how it should be applied.
- **Control enhancements:** Additional recommendations that 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.

AC-6 Control Details

AC-6	**Least Privilege**
	Control: Access should be minimal, and authorization is required for task completion.
	Discussion: Enforce processes, user roles, and privileges as necessary to achieve least privilege. The aim is to prevent over-permissioned access that could lead to unintended exposure or misuse of information.
	Control Enhancements: ● Role-based access to sensitive files. ● Automatic expiration of access rights. ● Logging and review of 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.

SECTION 3.0: CONCLUSION

3.1 Key Takeaways:

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

3.2 Security Implications and Recommendations:

- **Reinforce technical safeguards**: Implement automated link expiration, default to internal-only sharing, and restrict 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.