

Description of Compliance Breach Incident

Incident Overview

Date of Incident:

2024-05-18

Reported By:

Alice Johnson (Compliance Officer)

Location/System:

Human Resources Department / Employee Records Portal

Incident Description

On May 18, 2024, an employee accessed confidential personnel files without authorization via the internal Employee Records Portal. The access occurred over a 30-minute period and involved the viewing of records for 13 individuals not related to the employee's official duties. The breach was discovered during a routine audit of system access logs.

Policy/Regulation Breached

This incident constitutes a breach of the Company's Data Protection Policy, specifically Section 5.7 (Access to Confidential Information), as well as a violation of applicable privacy laws including the General Data Protection Regulation (GDPR) Article 32 (Security of Processing).

Immediate Actions Taken

- The employee's system access was suspended pending investigation.
- All affected individuals were notified of the unauthorized access.
- Incident reported to Data Protection Officer and HR Director.
- System audit initiated to assess extent of access and potential data leakage.

Root Cause Analysis

Preliminary analysis identified a lack of role-based access controls within the Employee Records Portal. The employee's user role inadvertently permitted access to a broader range of records than intended.

Corrective and Preventive Measures

- Role permissions updated and access restrictions enforced.
- Employee retraining on data privacy policies scheduled.
- Periodic access log reviews to be implemented quarterly.

Important Notes

- This document should be treated as confidential and shared only with authorized personnel.
- All facts must be recorded accurately and objectively.
- Timely reporting and documentation are critical for regulatory compliance.
- Review and update incident management procedures regularly.

