Systemwide Data Exposure Response Process [1]

The University of Colorado has a consistent, systemwide process for managing data exposure events. This process is a partnership between campus information technology departments, the Office of Information Security, University Counsel, Risk Management, communications teams, and other subject matter experts. Each area brings expertise to ensure that CU is fully investigating the event, meeting legal requirements, communicating effectively and improving processes to reduce the risk of future events.

This process and team make decisions and takes actions including determining the scope of the event, notifying affected individuals, notifying regulatory bodies, communicating with CU leadership, interacting with law enforcement, and identifying root causes for improvement efforts.

What is a Data Exposure Event?

A data exposure event is when personally identifiable information or other information protected under regulation is accessed or made available to unauthorized individuals. This could be a server that was attacked by a cybercriminal, an employee accidentally attaching the wrong file to an email, a lost/stolen device that wasn’t encrypted, or other events.

What should I do if I think a Data Exposure Event has occurred?

If you suspect a data exposure event might have occurred, please contact your campus information security team using the contact information on the side of this page. They will assess the event and, if appropriate, initiate the data exposure response process. The campus information security teams have access to a collaboration space containing the process documentation and templates.

Updated Sept. 15, 2023

Groups audience:
Office of Information Security
Right Sidebar:
Information Security Campus Contact

Links
[1] https://www.cu.edu/security/systemwide-data-exposure-response-process