AvePoint®
COMPLIANCE
GUARDIAN

Incident Management: Blocking Sensitive Information

Scenario

Bob, an accountant, uploads an expense report into the accounting site in SharePoint not realizing it contains the requester's credit card number.

Step 1

AvePoint Compliance Guardian immediately detects that there is PCI (Payment Card Industry) data within the file, classifies the document as "Restricted", encrypts it, and begins an incident workflow.

Bob receives a warning message that the document contains sensitive information, while Cornelius, the organization's Controller, receives an email indicating that a compliance incident has been assigned to him.

Step 2

Following the link in his email, Cornelius is brought to the Incident Management Center within AvePoint Compliance Guardian and sees that the document failed a PCI scan.

Step 3

After reviewing all of the details of the incident, including the specific violation and document permissions, Cornelius checks the audit history to make sure no one has accessed the document and deletes it directly from the incident report.

End Result

Your Users

Are able to work worry free knowing they are be able to easily meet compliance policies.

Your Compliance Team

Can easily generate reports on all violations across all content at any time and quickly remediate any outstanding issues.

Your Organization

Stays out of the headlines and avoids paying for costly data breaches.