



Microsoft Purview DLP

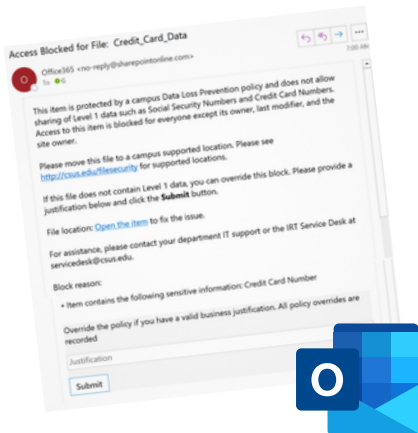
Ensuring Secure Storage & Sharing of Sensitive Data

1



Purview scans all faculty and staff campus files stored within Microsoft OneDrive and posted to Teams to determine if any files may contain Level 1 data that requires more secure storage.

2



If a file is identified, you'll receive an email from Office365 [<no-reply@sharepointonline.com>](mailto:no-reply@sharepointonline.com) alerting you about flagged file(s) including the file location and a link to the file.



To locate the flagged file quickly, login to Microsoft 365 with your Sac State credentials and type the file name into the search box.



If the file was flagged in error (a "False Positive") you can provide a justification within the email you received to override the flag.

3



Move your file(s) to the recommended secure location. Files containing Level 1 data must be stored on SacFilesSecure, or other recommended solution.

