Area of Responsibility:	Information Technology
Responsible Contact:	Chief Information Officer
Policy Identification:	Data Loss Prevention Policy
Effective :	07/01/2021
Last Revised:	04/26/2022

POLICY

The purpose of this procedure is to document activities that support appropriate and timely identification, monitoring, detection, and response to potential data loss incidents in Virginia Union University's environment.

The scope of this procedure includes activities related to monitoring and managing of internal and external security tools and third-party service providers that are related to incident detection processes. The IT function is responsible for implementing this procedure.

Data Loss Prevention (DLP) Procedures **POLICY**

The following sub-sections provide an Overview of DLP alerts configuration, monitoring and triaging/investigation and resolution procedures.

DLP Overview

Data Loss Prevention program is designed to detect and prevent loss of sensitive data in accordance with the Data Governance policy approved by the management.

DLP Alerting Policies Design & Configuration

DLP policies and design are based on classification of data identified in Data Governance Policy and requirements (key word lists) identified during discussions with key business stakeholders. Following alert rules are configured in O365 DLP module and email system:

Rule	Description
DLP Alerts	Generates an alert when an email containing defined set of keywords is sent outside the organization.
Detected Protected Attachments	Generates an alert when an email is sent outside the organization with a password protected attachment.
Mail Forwarding	Generates an alert when a mail forwarding rule to setup for an email account.

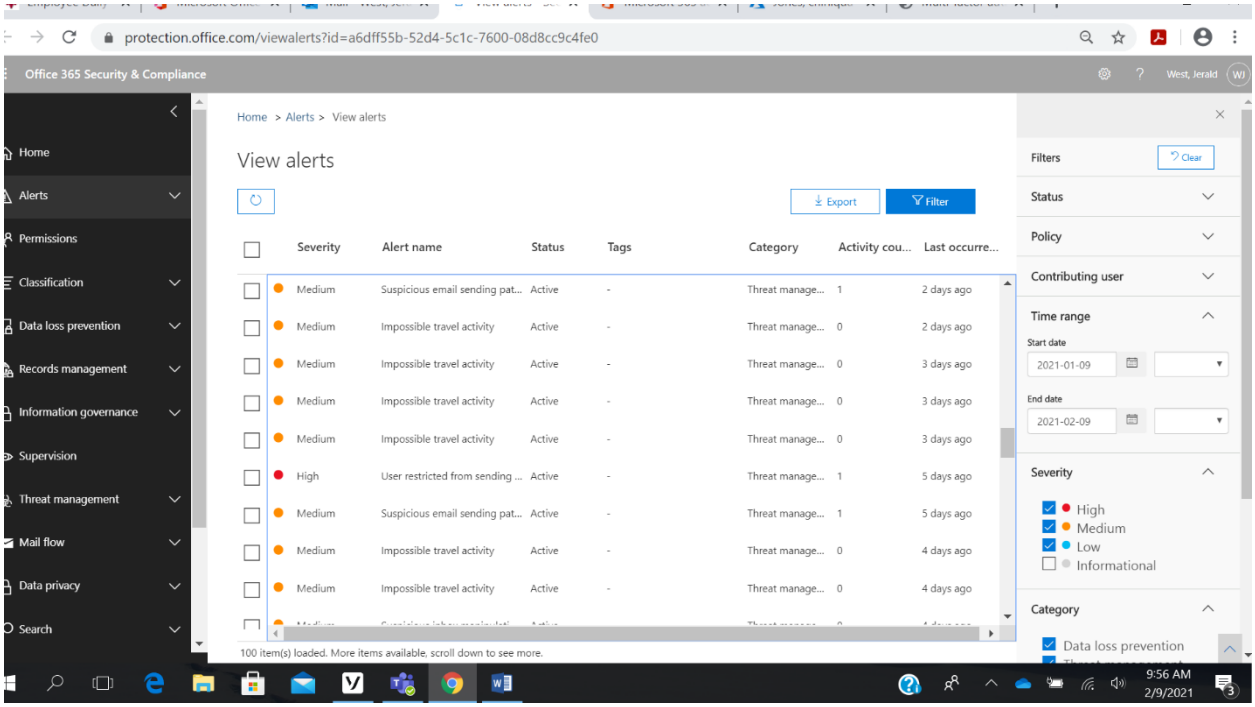
DLP Alert Monitoring, Investigation & Resolution

High Level Criteria for Triage:
DLP alerts are configured to send emails to IT, who will triage the alerts based on criteria such as amount and type of data transmitted, nature of external email addresses involved such as personal addresses, nature of the domains in email addresses, and actual names in email addresses involved in the alert.

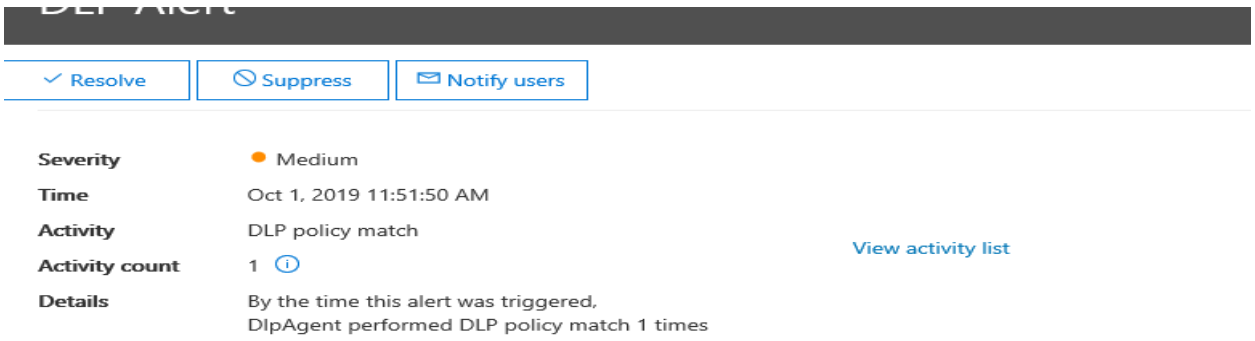
DLP Alerts are investigated using following steps:
(These are general guidelines only and does not cover every scenario, additional steps or procedures shall be used depending on the alert type and information available within the alert)

For DLP – Technology Group alerts:

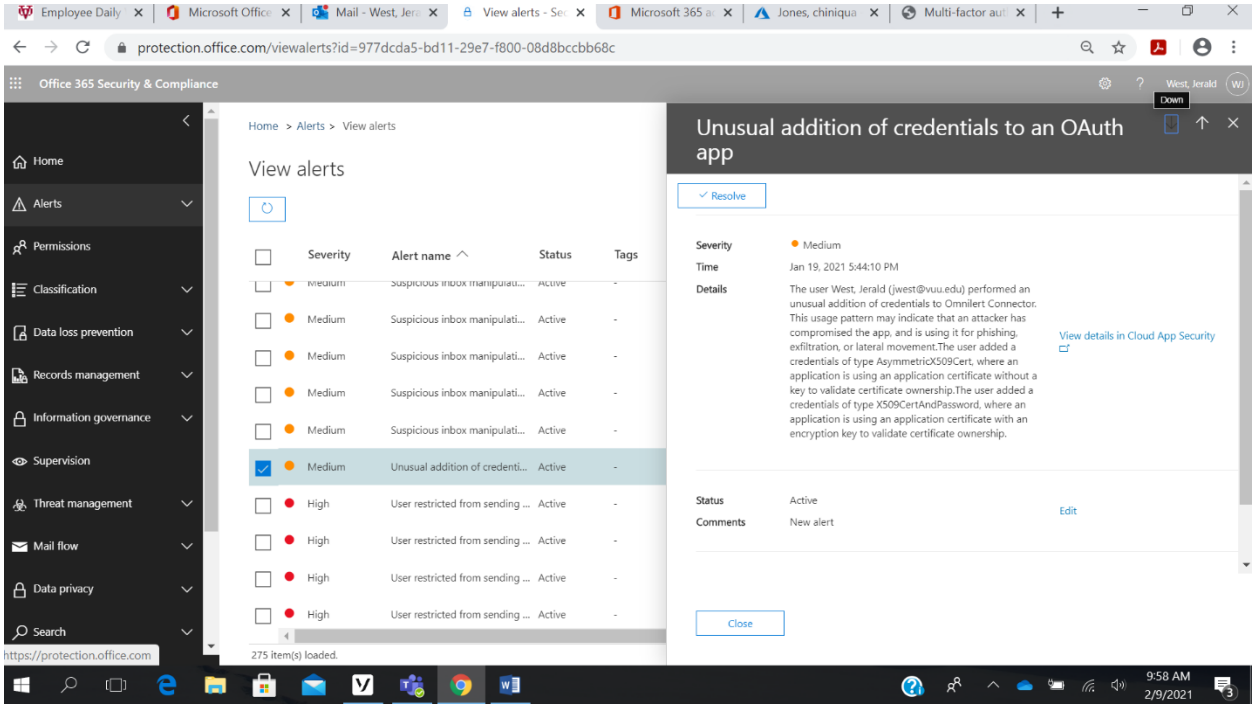
1. Choose the DLP Alert in question.



2. View the 'Activity List' and the DlpRuleMatch link to view the details of the alert.



3. Click on the arrow to view 'More Information'.



For DLP – Password Protected Attachment alerts:

If the alert meets any of the alert criteria IT will investigate the alert further. The decision is taken based on user's department (with special attention to HR & Legal), review of number of emails sent to this address etc. The issue will then be escalated to appropriate management / leadership team members for further investigation and action.

For Mail Forwarding alerts:

If the rules are setup to forward mails to external email address, the manager of the user is notified to confirm authorization, need and removal of the rule.

Follow-up and Resolution of Alert will be performed using following steps:

1. If required, reviewer will perform following actions to investigate the alert.
2. Email user's manager and cc' SR. DIRECTOR.
3. Inquire if the user was authorized to send data files.
4. Inquire if the company is a trusted-third party vendor.
5. Resolve the DLP Alert or escalate for further investigation, response and remediation steps as required if a data loss incident is identified.

Alert status will be set to one of the following depending up on the stage of review:

Active - New alert

Investigating - Alert is reviewed and determined that further investigation is required.

Dismissed - Alert is false positive and needs no further investigation.

Resolved – Investigation completed, and issue resolved.

Following resolutions will be used to document resolution of the alerts:

1. False positive - Internal communication to Virginia Union University employees (No further action).
2. False positive – Authorized data sent to a trusted third party (No further action).
3. False positive – Protected data sent to a trusted third party (No further action).
4. False positive – Authorized data sent to a personal email (No further action).
5. True positive – Unauthorized files or information sent to personal email. (Contact SR. DIRECTOR, and/or employee's manager by email.)
6. Custom categorization – Categorization used when reviewer needs to document special circumstances.

DLP Rule Configuration

The request, approval, and implementation procedures for adding, updating, or deleting the configuration of DLP rules are as below:

1. A request to add a new DLP rule configuration or update/delete an existing rule should be sent to DLP Approvers via email or through the ticketing system.
2. The DLP Approvers group will review and approve the DLP rule request based on the scope of the rule. For example, DLP alert rules are reviewed and approved by business owners identified. Other DLP rules such as password protected attachments and mail forwarding rules are reviewed and approved by the SR. DIRECTOR and/or IT Director.
3. DLP Security Administrators will review technical feasibility, test, and implement the request.
4. IT may add new rules to prevent data loss and/or for testing but will not remove or update existing rules without the approval of identified approvers. If a new rule is determined to be effective to prevent data loss, it will be formalized by IT.

Roles and Responsibilities Matrix

Group	Role	Description
DLP Approvers	VP & SR. DIRECTOR Sr. Director IT Director	Reviews and approves rule requests.
DLP Security Administrators	IT Director	Adds & tests new rules and config updates as per approved requests.

Documented Approvers:

_____	_____
Name, Title	**Date**
_____	_____
Name, Title	**Date**
_____	_____
Name, Title	**Date**
_____	_____
Name, Title	**Date**