Assignment 4: DLP Policy Statements

**Learning Objectives and Outcomes**

* You will gain insight into setting policy statements for DLP technology.
* You will learn how to draft appropriate response and actions to DLP alerts.

Assignment Requirements

You manager is worried about the lack of visibility into outgoing network traffic. The network team has recently deployed a Data Loss Prevention solution at the network perimeter, but it has not been configured yet. You have been tasked with creating the initial set of DLP policy statements and corresponding response procedures.

**Tasks**

Prepare a written report where you will recommend 3 unique DLP policy statements. 1 policy statement must represent a low level alert, 1 a medium level alert and 1 a high level alert. Each policy statement must include the following information at a minimum:

* What specifically triggers this alert
* What type of data is being transferred
* How is the data being transferred
* What additional information should be captured
* How is this alert categorized (must create your own scheme)
* What actions (minimum of 3) are required to respond to this alert

The type of data and response actions must be consistent with the corresponding alert level. In addition, provide one example of how someone could bypass the DLP technology and still exfiltrate the data without your knowledge.

**Submission Requirements**

* Format: Microsoft Word
* Citation Style: APA
* Length: 2 pages

Self-Assessment Checklist

* I created 3 DLP policy statements 1 for each alert level (Low, Medium, High)
* I included all 6 different policy elements
* I included 3 or more response actions per policy statement
* I created a scheme to categorize the different types of alerts
* I highlighted 1 technique to bypass DLP