# Configure DLP to Protect Sensitive Data from Being Used by ChatGPT

## Contents

## Introduction

This document describes how to use Data Loss Prevention (DLP) to protect sensitive data from being used by ChatGPT.

## Overview

The world of artificial intelligence is buzzing, with innovations like OpenAI's language model, ChatGPT, leading the charge. This AI powerhouse has been growing at a breakneck pace, transforming numerous industries with its smart, context-aware conversations. But with these exciting advancements come some potential challenges - specifically, data loss risks.

Think of ChatGPT as a super-smart conversation partner that generates text based on what you feed it. Now, if there is sensitive information in the mix and it is not handled properly, there is a risk of data breaches. This highlights why it is so important to have a comprehensive Data Loss Prevention (DLP) plan in place.

Your Umbrella DLP solution has been designed to shield your organization from these risks. Here are three pressing use-cases that our solution can help you address immediately and only take about 5-min to implement.

**A. Compliance with Data Privacy Regulations such as GDPR, HIPPA, and PCI-DSS:**

1. Head over to **Policies > Management > Data Loss Prevention Policy** in your Umbrella dashboard.
2. Start creating a new DLP rule. Simply click **Add Rule** at the top right-hand side and select **Real Time Rule**.
3. Give your rule a name that is easy to recognize, like 'ChatGPT Protection', and choose the severity level (anything from Low to Critical) that fits your needs.
4. In the **Classifications** section, pick one or more of the Built-In Compliance Classifications relevant to your organization. This could be the 'Built-in GDPR Classification' or 'Built-in PCI Classification', for example.
5. In the **Identities** section, select all the identities you wish to monitor and protect. If feasible, we recommend a wide selection for comprehensive coverage.
6. Move on to the **Destinations** section, select **Destination Lists and Applications for Inclusion**, and then pick **OpenAI ChatGPT**.
7. Now, it is time for action. In the **Action** section, you can choose to either **Monitor** or **Block**. If you a re new to this, we recommend starting with the 'Monitor' action. This allows you to observe usage patterns and make a more informed decision about the potential risks and benefits.
8. If you have chosen the 'Monitor' action, make sure to check out the DLP report after a week or a month. This shows you who is sharing sensitive information with ChatGPT and when, helping

you decide whether a 'Block' action is required.

**B. Protection of Personally Identifiable Information (PII):** To safeguard the PII in your organization from ChatGPT risks, just use the same instructions as above, but in step 4, select the 'Built-in PII Classification' instead of the compliance classifications.

**C. Protection of Source Code and Intellectual Property:** If your organization uses ChatGPT for activities involving source code or other intellectual property, use these steps:

1. First, create a new source code data classification. Navigate to **Policies > Management > Policy Components > Data Classification**. Click the **Add** button on the top right-hand side and give your data classification a recognizable name, like 'Source Code Classification'.
2. Choose **Source Code** from the list of **Built-in Data Identifiers**.
3. Click **Save**.
4. After saving, revisit the instructions for 'Compliance with Data Privacy Regulations' above, but in step 4, choose your newly created Source Code Data Classification instead of the built-in ones.

The process is straightforward and only takes a few minutes of your time, but the benefits to your organization's security and compliance is invaluable. We urge you to take these steps as soon as possible to fortify your data protection.

Want to learn more about Generative AI risks and how Umbrella can protect you, watch the webinar Protect Your Sensitive Data from ChatGPT Usage.