Standard PR.DS: PII Data Loss Prevention – Microsoft Office 365

February 11, 2021

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **OCIO_IAS@ed.gov**

APPROVAL

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2021.02.11 12:43:48 -05'00'

_____ _____

Steven Hernandez **Date**

Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Draft Date	Summary of Changes
1.0	3/18/2020	Initial draft
1.1	4/1/2020	References to “long-dash” format removed from Sections 5.1.1 and 5.1.4
1.2	5/5/2020	Added section 5.2 DLP (SharePoint Online)
1.3	2/9/2021	Reviewed for accuracy and timeliness. Standardized Risk Acceptance and Policy Exception section and updated references in Appendix A.

Table of Contents

1 Purpose

This document establishes the Department standards for safeguarding Personally Identifiable Information (PII) within Microsoft Office 365 (O365) programs. This document supersedes any prior documentation establishing such a standard.

2 Applicability

The standard established in this document applies to all employees, contractors, and users authorized to access ED information systems, systems operated or maintained on behalf of ED, or ED information.

3 Scope

This document details the minimum data loss prevention (DLP) requirements the Department must follow to prevent the intentional or accidental exposure of Personally Identifiable Information (PII) to unauthorized parties. Specifically, this document establishes standards for the following:

- How Microsoft Exchange and SharePoint Online should identify PII, specifically Social Security numbers (SSNs) and credit card numbers
- The SSNs and credit card number formats that are to be detected
- Conducting DLP overrides

4 References

The following sources are referred to in this standard:

- **Microsoft 365 - Data Loss Prevention**: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies

5 Requirements

The O365 DLP setting used by the Department must be able to identify the following types of PII within the Exchange Server and SharePoint Online:

- Social Security numbers (SSNs)
- Credit Card numbers

5.1 DLP (Microsoft Exchange)

5.1.1 SSNs

The Microsoft Exchange DLP setting must identify SSNs contained within outgoing email traffic (ED user to non-ED user) as PII. The DLP setting must identify SSNs written in the following format:

- XXX-XX-XXXX (short dash)

When an SSN is included in the body of an outgoing email (to a non-ED user), the following warning message (shown in Figure 1 below) will appear on the ED user's email **before** the email is sent:

- Policy Tip: An email or attachment which may contain unencrypted sensitive PII information was detected. You can override now or send your email by encrypting using a PIV card or as an attachment using WinZip.
- **X** isn't authorized to receive this type of information.
- To send this message without removing the information, ***you must first click override***. **[See Figure 1, below]**
- The following recipient is outside your organization: **X**

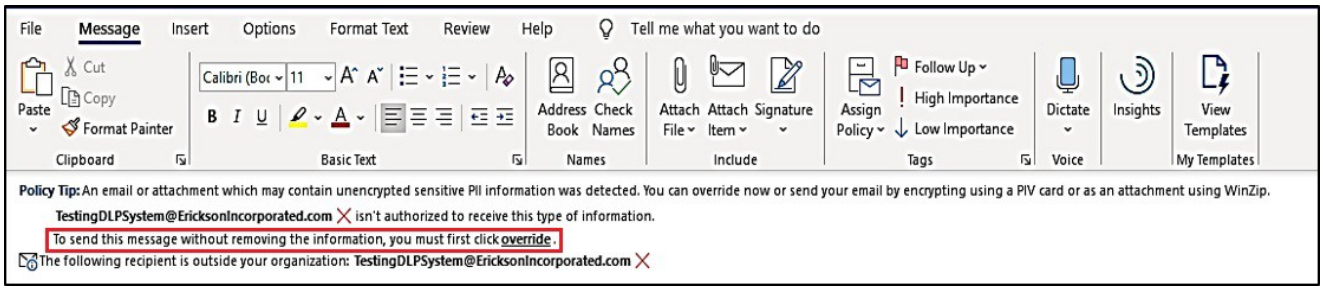

Figure 1: Email Warning Message

5.1.2 Credit Card Numbers

The Microsoft Exchange DLP setting must identify credit card numbers contained within outgoing email traffic (ED user to non-ED user) as PII. The DLP setting must identify credit card numbers written in the following 16-digit format:

- XXXXXXXXXXXXXXXX

When a credit card number is contained within the body of an outgoing email (from an ED user to a non-ED user), the message in Figure 1 must appear on the ED user's email **before** the email is sent.

5.1.3 Justifications for Overrides

The following types of PII overrides must be available within the Exchange Server. These overrides are:

- **For a business justification**

  If an ED user must send an email that contains an SSN to a non-ED user, they must provide a business justification. If the override is business-justified, the ED user must provide an explanation detailing their reason for the override (see Figure 2).

- **For a DLP false positives**

  If the DLP setting identifies information in the outgoing email as an SSN, but the information is not an SSN, the ED user must deem this a 'false positive' and conduct the necessary override (see Figure 2).

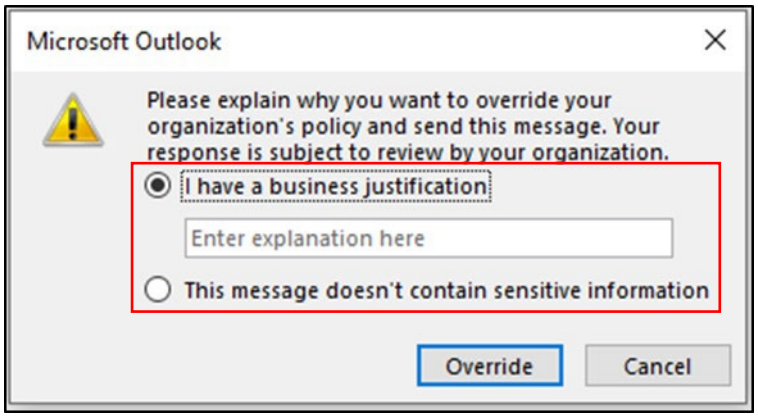

Figure 2: Outlook Overrides (Business Justification and False Positive)

- **For the following exceptions:**

  - PII exceptions covered under the 1974 Privacy Act (e.g., users are authorized to send their own PII to themselves.) See https://www.justice.gov/opcl/ten-exemptions.

  - Where the user has 100% certainty that at minimum, the Department-mandated level of encryption is in use. ED's mandated minimum level of encryption is Transport Layer Security (TLS) 1.2. DLP (Microsoft SharePoint).

5.2 DLP (SharePoint Online)

5.2.1 SSNs

The Microsoft SharePoint DLP setting must identify SSNs contained within documents being uploaded to SharePoint. The DLP setting must identify SSNs written in the following format:

- XXX-XX-XXXX (short dash)

Additionally, there must be a qualifier (i.e., "SSN" or "Social Security") mentioned within 300 characters of the actual SSN.

5.2.2 Credit Card Numbers

The Microsoft SharePoint DLP setting must identify credit card numbers contained within documents being uploaded to SharePoint. The DLP setting must identify credit card numbers written in the following 16-digit format:

- XXXXXXXXXXXXXXXX

Additionally, there must be a qualifier (i.e., “credit card”) mentioned within 300 characters of the actual SSN.

5.2.3 Overrides

Overrides are not required to be available on SharePoint Online.

6 Risk Acceptance/Policy Exceptions

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department’s Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

APPENDIX A: RESOURCES AND REFERENCES

- OM:6-104: *The Privacy Act of 1974*
- OM:6-108: *Privacy: Section 208 of the E Government Act of 2002*