# SOP - Email Security with Proofpoint

## 1. Purpose

The purpose of this Standard Operating Procedure (SOP) is to establish clear guidelines and procedures for managing, monitoring, and responding to email security threats using the Proofpoint Email Security Platform. This SOP aims to protect the organization's email infrastructure, sensitive data, and users from various email-borne attacks, including but not limited to phishing, malware, spam, and Business Email Compromise (BEC) attempts, while ensuring compliance with relevant data protection policies and regulations.

## 2. Scope

This SOP applies to all employees, contractors, and third parties who manage or interact with the organization's email system protected by Proofpoint. It specifically covers the use and administration of the Proofpoint Email Protection (PEP), Proofpoint Targeted Attack Protection (TAP), Proofpoint Information Protection (Encryption), and Proofpoint Security Awareness Training (PSAT) modules, where applicable.

## 3. Definitions and Abbreviations

- **Proofpoint:** Refers to the Proofpoint Email Security and Compliance Platform.
- **PEP (Proofpoint Email Protection):** Core email gateway for spam, virus, and content filtering.
- **TAP (Targeted Attack Protection):** Advanced threat protection for sophisticated attacks like URL rewriting, attachment sandboxing.
- **BEC (Business Email Compromise):** A scam targeting businesses that perform wire transfer payments, often using spoofed email addresses.
- **Phishing:** Attempts to obtain sensitive information (e.g., usernames, passwords) by masquerading as a trustworthy entity in an electronic communication.
- **Malware:** Malicious software (e.g., viruses, ransomware) designed to disrupt, damage, or gain unauthorized access to computer systems.
- **Quarantine:** A holding area for suspicious emails that require review before delivery or rejection.
- **False Positive:** A legitimate email incorrectly identified as a threat by Proofpoint.
- **False Negative:** A malicious email that Proofpoint failed to detect and block.

- **SLA (Service Level Agreement):** Defines the level of service expected by a customer from a supplier.
- **IOC (Indicator of Compromise):** Forensic evidence of a potential intrusion or attack.
- **URL Rewriting/Wrapping:** Proofpoint's feature to change URLs in emails to protect against malicious links by routing them through a Proofpoint sandbox.
- **Sandbox:** A secure, isolated environment where suspicious email attachments or URLs are executed and analyzed for malicious behavior without affecting the live network.
- **PSAT (Proofpoint Security Awareness Training):** Proofpoint's integrated security awareness training platform.

## 4. Roles and Responsibilities

- **Chief Technology Officer (CTO):**
  - Overall accountability for email security strategy and policy.
  - Approves significant Proofpoint configuration changes and incident response plans.
  - Ensures compliance with regulatory requirements.
- **IT Security Specialist:**
  - Weekly monitoring and triage of Proofpoint alerts and quarantines.
  - Investigates and responds to email security incidents.
  - Manages Proofpoint policies, rules, and configurations.
  - Performs regular health checks and maintenance of the Proofpoint platform.
  - Provides Level 2/3 support for email security-related issues.
  - Generates security reports.
  - Provides network and infrastructure support for Proofpoint integration.
  - Assists with email routing and mail flow issues.
  - Provides Level 1 support for general email issues (e.g., email not delivered, user quarantine access).
  - Collaborates on employee awareness training content.
  - Provides guidance on data privacy and compliance matters related to email content and retention.
- **All Employees:**
  - Adhere to email security policies.
  - Report suspicious emails using the designated reporting mechanism.
  - Participate in security awareness training.

## 5. Policy Statement

All organizational email communications are subject to inspection and protection by the Proofpoint Email Security Platform. The organization is committed to maintaining a secure email environment, protecting sensitive information, and providing a robust defense against email-borne threats. All email security incidents will be handled according to this SOP and the organization's broader Incident Response Plan.

## 6. Procedures

### 6.1. Weekly Monitoring and Alert Review

**Objective:** Proactively identify and address potential email threats.

**Frequency:** Weekly, on a Friday morning, and potentially ad-hoc during critical alerts.

**Steps:**

1. **Access Proofpoint Admin Console:** Log in to the Proofpoint dashboards(Login).
2. **Review Dashboards:**
    a. **Dashboard:**
        i. Check for significant spikes in blocked spam, viruses, or policy violations over the past 30 days.
        ii. Review "Threat Overview" and "Threat Traffic."
        iii. Look for any mail flow alerts or system health warnings that occurred during the week.
3. **Quarantine Review**
    a. Access the **Spam Detection -> Quarantine** section.
    b. Review emails quarantined as "Malware," "Phishing," or high confidence "Spam" for the past week.
    c. For each suspicious email:
        i. Examine sender, subject, attachments, and embedded URLs.
        ii. Determine if it's a legitimate email (False Positive) or a genuine threat.
        iii. **Action:** Release (if legitimate), Delete, or Report to Proofpoint (if new threat variant).
    d. **Note:** End-user quarantine review processes (where users manage their own low-confidence spam) are out of scope for this SOP but should be supported.
4. **System Health Check:**

    a. Verify Proofpoint services are running.
    b. Review system logs for errors or warnings not directly related to email traffic, focusing on weekly anomalies.
5. **Document Anomalies:** Record any significant findings, unusual patterns, or critical alerts identified during the weekly review in the security incident log.

## 6.2. Incident Response for Email Threats

**Objective:** Provide a structured approach to identifying, containing, eradicating, recovering from, and analyzing email security incidents, maximizing the advanced capabilities of our Proofpoint enterprise license.

**General Incident Response Flow:**

1. **Detection & Triage:** Identify a potential incident via Proofpoint alerts, user reports, or internal monitoring.
2. **Analysis & Validation:** Verify the authenticity and scope of the threat. Is it true positive? Who is affected?
3. **Containment:** Take immediate action to stop the spread (e.g., block sender, quarantine email, remove from inboxes).
4. **Eradication:** Eliminate the threat (e.g., clean infected systems, remove malicious content).
5. **Recovery:** Restore affected systems/users to normal operations.
6. **Post-Incident Activity:** Document, analyze lessons learned, and update policies/procedures.

### 6.2.1. Phishing/Malware Detection

**Source of Detection:** Proofpoint TAP alerts, Proofpoint PEP quarantine, User-reported suspicious emails (Phish Alarm). **Our enterprise TAP license provides deep insights into these advanced threats.**

**Steps:**

1. **Initial Assessment:**
    a. **Proofpoint Alerts:** If an alert is triggered, go directly to the Dashboard for detailed analysis powered by TAP's advanced sandboxing and URL defense.

b. **User Reports:** If a user reports an email via the Phish Alarm button, check the Threat Protection > User Reported Suspect Email queue. These user reports feed directly into our enterprise threat intelligence.

2. **Detailed Analysis (Message Log):**
    a. Examine the email headers, body, attachments, and URLs.
    b. Review Proofpoint's Verdict.
    c. Check for similar emails sent to other users in **Message Log**.
    d. **For URLs:** Investigate the rewritten URL. Has anyone clicked on it? Check the "URL Clicks" section in dashboard, understanding that TAP's URL defense has already provided an initial layer of protection.
3. **Containment & Eradication:**
    **a. Quarantine/Block:** If confirmed malicious, ensure the email is quarantined or blocked. If it reached an inbox, use **Message Remediation** to search and remove all instances from user inboxes. **This powerful remediation tool is a key feature of our enterprise license.**
    b. **Block Sender/Domain:** Add the malicious sender's email address or domain to the Proofpoint Block List.
    c. **Block Malicious URLs/IPs:** If a malicious URL or IP is identified, consider adding it to the organization's firewall/proxy block lists.
    d. **Force Password Reset:** If credentials are suspected to be compromised due to a phishing link click, initiate an immediate password reset for the affected user.
4. **User Notification & Awareness:**
    a. Notify the affected user(s) about the incident.
    b. If a widespread phishing campaign is successful, issue an internal security alert to all users.
    **c.** Use **PSAT(Proofpoint Security Awareness Training)** to assign targeted training modules to affected or vulnerable users, **leveraging our enterprise PSAT platform for tailored education.**
5. **Documentation:** Record the incident details, actions taken, and affected users in the Incident Management System.

### 6.2.2. BEC (Business Email Compromise) Prevention & Response

**Objective:** Protect against and respond to sophisticated financial fraud attempts, making full use of **Proofpoint's enterprise-grade Imposter Defense capabilities.**

**Prevention Focus (Proofpoint):**

1. **Imposter Defense:** Ensure Imposter Defense policies are configured to detect look-alike domains, display name spoofing, and reply-to address manipulation. **This advanced protection is a hallmark of our enterprise TAP license.**
2. **Internal Mail Protection:** Apply Proofpoint internal mail policies to detect anomalous internal email behavior or compromised internal accounts.
3. **User Education:** Regular **PSAT** training on BEC indicators, **reinforced by real-world examples from our Proofpoint detections.**

**Response Steps for Suspected BEC:**

1. **Immediate Verification:** Do NOT respond to the email. Directly contact the purported sender via a **known, pre-verified phone number** or separate communication channels to verify the request. Do NOT rely on contact information provided in the suspicious email.
2. **Isolate & Analyze:**
    a. Quarantine the email if it's still in the system.
    b. Analyze the email headers and content for spoofing techniques (e.g., subtle domain variations, reply to mismatches, display name spoofing).
    c. Leverage **Proofpoint's Imposter Detection details**, provided by our enterprise TAP license.
3. **Remediation:**
    c. Remove all instances of the BEC email from user inboxes using Proofpoint's Message Remediation feature.
    d. Add sender/domain to the Proofpoint **Block List** if it's a known malicious actor.
4. **Post-Incident Review:**
    a. Analyze how email bypasses existing controls.
    **b.** Adjust Imposter Defense policies in Proofpoint as necessary, **fine-tuning our enterprise protection.**
    c. Reinforce user training on BEC awareness.

5. **Documentation:** Record detailed incident information, including financial implications, in the Incident Management System.

### 6.2.4. Handling False Positives

**Objective:** Ensure legitimate emails are delivered promptly without compromising security, while **continuously refining our Proofpoint enterprise controls.**

**Source of Detection:** User reports ("My email didn't arrive"), IT Operations/Helpdesk tickets, Weekly Quarantine Review.

**Steps:**

1. **Verify Legitimacy:**
    a. Review the email in Proofpoint's **Message Log** (Mail Flow -> Message Log).
    b. Check why it was blocked/quarantined (e.g., spam score, content filter, attachment type).
    c. Communicate with the sender/recipient to confirm the email's legitimacy.
    d. Examine sender reputation, SPF/DKIM/DMARC status.
2. **Determine Action:**
    a. **Release:** If clearly legitimate, release the email from quarantine.
    b. **Add to Safelist (Allow List):** For frequently occurring legitimate senders/domains that are repeatedly flagged, consider adding them to Proofpoint's **Sender IP/Domain Reputation -> Safelist**. Use caution and restrict to specific senders/recipients if possible, rather than broad domain safe listing.
    **c. Adjust Policy:** If a specific content filter or rule is consistently generating false positives for legitimate business communication, review and adjust the rule's sensitivity or conditions. **Our enterprise license allows granular control for such fine-tuning.**
3. **Educate Users/Senders:**
    a. Inform the user why the email was blocked and how it was resolved.
    b. Advise external senders to check their email configuration if their emails are consistently flagged.
4. **Monitor:** After making adjustments, monitor the Message Log to ensure the issue is resolved and no new false positives occur from the same source.
5. **Documentation:** Record false positive incidents and the resolutions for future reference and policy refinement.

## 6.5. Reporting and Metrics

**Objective:** Measure email security effectiveness and identify trends, **utilizing the comprehensive reporting capabilities of our enterprise Proofpoint platform.**

**Frequency:** Weekly

**Steps:**

6. **Generate Standard Reports:**
    a. **Weekly:**

i. **Threat Report:** Number of blocked spams, malware, phishing, BEC attempts.
ii. **Targeted Attack Summary:** Top attacked users/departments, top campaigns, URL click rates. **These granular reports are a benefit of enterprise TAP.**
iii. **Message Activity Report:** Overall mail flow statistics (inbound/outbound, delivered vs. blocked).

b. **Quarterly:**
i. Trend analysis of threat types and volumes.
ii. Effectiveness of policy changes.
iii. False positive/false negative rates.
iv. User behavior insights from PSAT (phishing click rates, training completion), available through our enterprise PSAT module.

7. **Review and Analyze:**
a. Identify emerging threats or patterns.
b. Assess the effectiveness of current security controls.
c. Determine areas for policy refinement or user training.
8. **Distribute Reports:** Share relevant reports with management, CISO, and other stakeholders.
9. **Actionable Insights:** Translate report findings into actionable recommendations for improving email security posture.

## 6.6. User Training and Awareness

**Objective:** Empower users to be the first line of defense against email threats, **leveraging our full enterprise PSAT license for continuous education.**

**Frequency:** Ongoing, initial training for new hires, refresher training bi-annually, targeted training as needed.

**Steps:**

10. **Initial Onboarding Training:**
a. Educate new hires on email security best practices, the importance of reporting suspicious emails (Phish Alarm), and the organization's email policy.
11. **Regular Security Awareness Training (PSAT):**
**a.** Utilize **Proofpoint Security Awareness Training (PSAT)** modules to deliver continuous education on phishing, BEC, malware, and data

handling. **Our enterprise license provides access to a rich library of training content.**

**b.** Conduct simulated phishing campaigns (using **PSAT**) to test user awareness and identify vulnerable individuals. **The advanced capabilities of enterprise PSAT allow for highly customized and realistic simulations.**

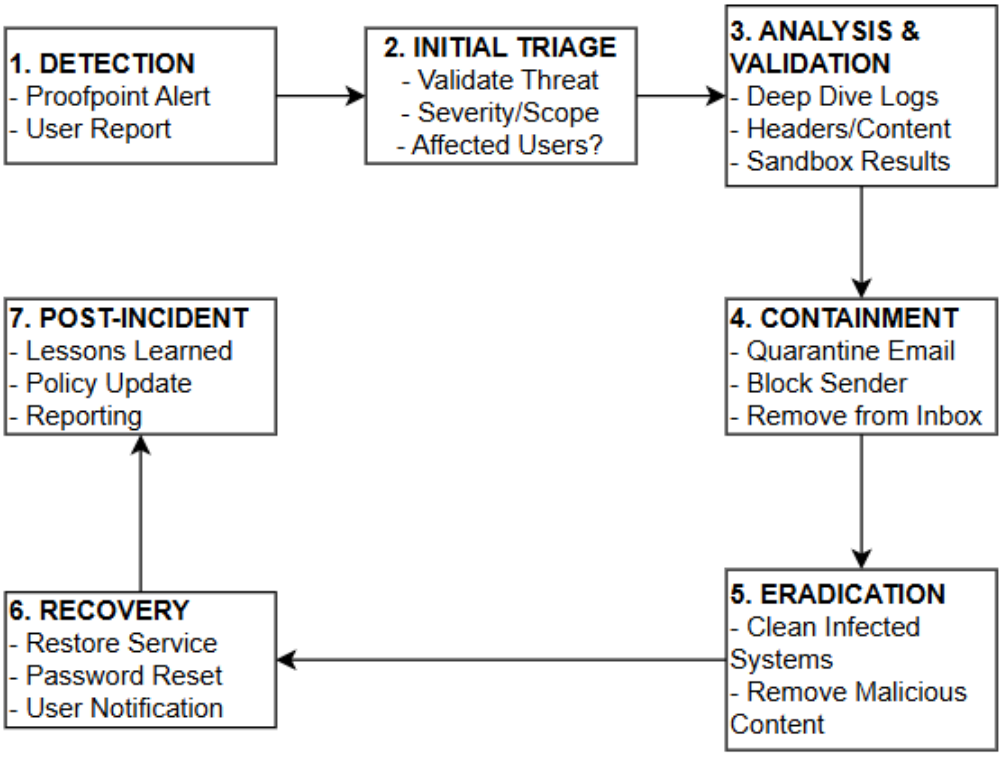
c. **Note:** Link PSAT training assignments to phishing simulation failures.

12. **Phish Alarm Button Promotion:**
    a. Regularly remind users about the Phish Alarm button (Proofpoint's Email Reporting feature) and its importance.
    b. Communicate the feedback process for reported emails.
13. **Incident-Specific Communications:**
    a. After significant email security incidents, send out targeted communications to affected users or the entire organization to raise awareness about the specific threat.
14. **Review Training Effectiveness:**
    **a.** Monitor PSAT metrics (completion rates, click rates on simulations, reported email volume) to assess the impact of training programs, **using the analytical tools available in enterprise PSAT.**

# 9. Appendix

### Appendix A: Email Security Incident Response Workflow

**(Flowchart/Diagram - Conceptual)**




## Appendix B: Proofpoint Threat Categories Glossary

- **Spam:** Unsolicited bulk email.
- **Phishing:** Attempts to trick users into revealing sensitive information via fraudulent websites or credential harvesting.
- **Malware:** Emails containing malicious attachments (executables, scripts, documents with macros) or links to malware downloads.
- **Imposter:** Emails impersonating a known sender (e.g., CEO, vendor, HR) often for financial fraud (BEC).
- **Bulk Mail:** Legitimate, but often unwanted, marketing or newsletter emails (can be configured to be treated differently than spam).
- **Exploit Kit:** Emails leading to web pages hosting exploits that target browser or plugin vulnerabilities.
- **Sensitive Content:** Emails flagged by DLP policies containing specific patterns (e.g., credit card numbers, SSN, PII).

**Date: 06/16/2025**