Stratos Cyber

AI-PHISHING RESPONSE & VERIFICATION PROTOCOL

(Governance & Policy Insert – August 2025)

PURPOSE

The purpose of this protocol is to establish a clear and enforceable standard for validating communications that may involve sensitive data, financial transactions, or privileged access. The growth of AI-powered phishing and executive impersonation requires organizations in the Caribbean to adopt layered verification processes that cannot be bypassed by linguistic deception, spoofed identities, or synthetic voice content.

SCOPE

This protocol applies to all staff, contractors, and third parties who initiate, receive, or approve communications related to:

- Financial transactions (payments, wire transfers, vendor account changes)
- Authentication or credential resets
- Requests for access to sensitive systems or regulated data
- Authorizations for procurement, contract awards, or HR actions

*This protocol will be reviewed annually or upon significant changes to the regional threat landscape, as assessed by the CISO or equivalent authority.

Stratos Cyber

POLICY REQUIREMENTS

1. Secondary Channel Validation
All high-risk requests must be verified through a secondary, trusted channel. For example:

- A phone call to a verified number on file (not the number contained in the suspicious message).
- In-person confirmation where feasible.
- Secure messaging platforms pre-approved by the organization.

2. Prohibited Practices
Employees must not:

- Approve requests solely on the basis of email or instant messaging.
- Use the reply function, contact details, or links embedded within the suspicious message for verification.

3. Escalation
If a request cannot be validated, or if anomalies remain after validation, the employee must escalate to the designated Information Security Officer or equivalent. Escalation is mandatory regardless of the role or seniority of the purported sender.

4. Recordkeeping

- All validation actions must be logged and retained for a minimum of twelve (12) months.
- Suspicious communications must be preserved and forwarded to IT Security for forensic review.

5. Awareness and Enforcement

- This protocol must be communicated to all staff annually, with mandatory acknowledgment.
- Compliance with this protocol will be monitored through internal audits. Failure to comply may result in disciplinary measures under organizational policy.

Stratos Cyber

ABOUT US

Stratos Cyber is a leading innovator in cybersecurity, dedicated to helping businesses navigate an ever-evolving digital threat landscape.

Headquartered in Canada with a global reach, we specialize in delivering tailored security solutions that empower organizations to safeguard their digital assets, maintain compliance, and build resilience against future threats.

With a strong focus on innovation and governance, we leverage cutting-edge technology and a proactive approach to ensure our clients thrive in today's connected world.

Email

info@stratos-cyber.com

Telephone

+1 514 299 2015

Website

www.stratos-cyber.com