TECHNOLOGY SOLUTIONS

Technology Solutions – External Email Identification & Handling

Department: Technology Solutions
Procedure Name: External Email Identification & Handling
Procedure ID: TS-PROC-016
Effective Date: 01/22/2026
Last Reviewed: 01/22/2026

Owner: Chief Information Officer (CIO)

Applies To: All HGTC faculty, staff, contractors, and Technology Solutions personnel

1. Purpose

This procedure increases awareness of external email communications and reduces the risk of phishing, fraud, credential compromise, and social engineering attacks by clearly identifying emails originating from outside the institution.

2. Scope

This procedure applies to all email delivered to HGTC email systems and all users accessing institutional email.

3. External Email Identification

HGTC has implemented an external email warning banner that appears on messages originating from outside the institution. The banner serves as a visual indicator prompting recipients to exercise additional caution.

4. User Responsibilities

- Exercise heightened caution when viewing external emails
- Verify the sender before responding or acting
- Be alert for urgent language, unexpected requests, links, or attachments

5. Prohibited Actions

- Clicking links or opening attachments without verification
- Providing passwords, MFA codes, or sensitive information
- Approving financial or account changes based solely on email
- Bypassing security warnings or banners

6. Reporting Suspicious Emails

All suspicious external emails must be reported promptly using approved reporting methods to allow Technology Solutions to investigate and respond.

7. False Positives & Business Impact

Legitimate external emails are expected. Users are encouraged to verify communications rather than ignore them.

8. Training & Awareness

External email awareness is reinforced through security training and simulated phishing exercises.

9. Exceptions

Exceptions to this procedure require CIO approval and must be documented and reviewed periodically.

10. Compliance & Enforcement

Failure to follow this procedure may result in security review or corrective action. This procedure is governed under TS-PROC-001.

11. Review Cycle

This procedure will be reviewed annually or as threat patterns or institutional needs change.