The Heritage Group

7.17 IT Security Policy

This Information Technology (IT) Security Policy (Policy) applies to all employees and contractors of The Heritage Group and its operating companies (THG) who have a company-issued email address. IT security focuses on protecting THG's computers, networks, programs and data from unauthorized access and damage. Violations of this Policy and the associated IT security protocols will result in disciplinary measures as provided herein.

1. **IT Security Awareness Training.**
    a. The IT Shared Services (ITSS) division of THG will assign IT security awareness training to users at a cadence that ITSS deems appropriate (usually annually). Users determined by ITSS to be higher risk will receive additional training assignments, as needed. Higher-risk populations include users with access to payroll, financial and accounting systems; users with access to sensitive HR data; company officers and their administrative personnel; and/or users that have higher frequencies of attack.
    b. For all training assignments, regardless of a user's high- or low-risk status:
        i. Users will receive system-generated notices about and reminders to take the assigned training.
        ii. Failure to complete assigned training within the allotted time frame will result in the disabling of access to THG's IT systems unless and until the required training is completed.
        iii. Supervisors of each user who fails to complete any training within the required timeframe will be notified directly.
        iv. Repeated noncompliance with this provision will be deemed an act of insubordination and will result in suspension without pay or termination.

2. **IT Security Tests.** All users to whom this Policy applies will receive quarterly "phishing" prompts that are designed to test a user's awareness of and compliance with THG's IT security protocols. Users who fail such tests will be addressed as follows:
    a. Failure 1: The user, user's supervisor, user's appropriate IT leader, and user's HR Business Partner (HRBP) will be notified, and cybersecurity training will be assigned and completed within 48 business hours after (i) the failure, or (ii) returning to work from an excused absence (e.g., a user is on leave, taking scheduled PTO, etc.). If the training is not completed as provided, ITSS will disable the user's access until the training is completed.
    b. Failure 2: A second failure within the same 12-month period as Failure 1 will result in the same actions as set forth in 2.a. above, plus:
        i. the user's access to the Internet (other than approved, business-necessary cloud-based solutions) will be shut off for 90 days; and
        ii. the user and the user's supervisor will be required to complete five (5) additional cybersecurity training modules in the 30-day period that follows.
        iii. the user's HRBP will provide the user a written warning and the written warning will be added to the user's HR file.
    c. Failure 3: A third failure within the same 12-month period as Failures 1 and 2 will result in the following actions:
        i. ITSS will immediately suspend the user's access to THG's network, and notify the user's supervisor, the user's appropriate IT leader, the applicable HRBP, and user's business president (or equivalent);
        ii. the user's access will not be restored unless and until the user completes related training within one (1) hour of losing access due to the third failure;

iii. the user's access to the Internet (other than approved, business-necessary cloud-based solutions) will be shut off for one (1) year;
iv. the user and the user's supervisor will be required to complete 5 additional cybersecurity training modules in the 30-day period that follows; and
v. the user's supervisor and the HR business partner will be required by this Policy to implement additional disciplinary action under this Section 2.c., up to and including a reduction in the user's annual bonus eligibility.

d. Additional Failures: More than 3 failures within the same 12-month period will be escalated to the president (or equivalent) of the applicable THG company who will be required by this Policy to implement additional disciplinary action, up to and including suspension without pay and termination. The user, user's supervisor, user's appropriate IT leader, and the user's HRBP will also be notified.

3. **Inputting Credentials.** ITSS has tools in place that detect when a user inputs credentials into non-company and potentially malicious websites.
   a. If ITSS tools detect a user inputting credentials into such sites:
      i. the user's access to the THG network and email will be suspended immediately;
      ii. to regain access, the user must complete related training within one (1) hour after ITSS re-enables access;
      iii. the user's access to the Internet (other than approved, business-necessary cloud-based solutions) will be shut off for one (1) year;
      iv. the user will be required to complete five (5) additional cybersecurity training modules in the 30-day period that follows; and
      v. the user's supervisor and the HRBP will have a counseling session with employee.
   b. If ITSS tools fail to detect a user inputting credentials into such sites and a security breach results, the matter will be escalated to the president of the applicable THG company who will be required by this Policy to implement appropriate disciplinary action, up to and including suspension without pay and termination.

4. **Do Your Part.** Every user is empowered to protect THG's IT. Users should report suspected email-based cyber threats to ITSS via the "Report Phish" button in Outlook, or by forwarding any suspicious email or IT activity to the ITSS Service Desk. Each quarter, as a way to recognize those of you doing your part, ITSS will review all legitimate phishing or other potential IT security issues reported and award three (3) $50 gift cards to individuals selected at random from all users.

Effective October 2024