

## Purpose & Approval

- Purpose:
  - The penetration test and corresponding risk assessment will be performed by G&G industries to test the adequacy and effectiveness of security control measures in place to protect the security and integrity of sensitive information technology (IT) systems and data.
- Approval:
  - Approved by: Cornelius Carbonimus (System owner)

## Scope

- External Network penetration test
  - Up to 200 IP's
- Internal network penetration test
  - If no access can be gained during the external/social engineering activities after one week, we'll move to a breach attack
- Social Engineering activities:
  - Spear Phishing
  - Pre-text phone calling
  - Physical security assessment
    - Can be during the day or evening
    - Talk your way into areas, limited physical bypass
    - Attempt to gain internal network access
    - Attempt to gain network access to facilitate persistent access
    - G&G Industries will leave behind malicious devices
  - Wireless vulnerability assessment
- Authorization:
  - The testing team is explicitly permitted to perform only the activities described here.
  - Authorized by Cornelius Carbonimus.

### Authorization statement:

By signing below, Gary Fulstetter is authorized to begin testing and conduct the activities listed in the scope above during the agreed upon dates and hours. The authorization is null if any activities or information outside of what is authorized in this experiment.

Signature X \_\_\_\_\_

## Timing & Deconfliction

- Engagement:
  - Testing can only be performed between 2025/10/2 - 2025/10/16
  - Testing can also only be performed during business hours of 9AM - 6PM
  - No testing cannot be performed during critical business period or maintenance freezes

**Communications & Escalation:**

- POC: Cornelius Carbonimus, System Owner, 740-592-3106, CarbonimusC@gmail.com
- Backup: Andrea DeGranus, [DegranusA@gmail.com](mailto:DegranusA@gmail.com), 740-592-9835
- Tester: Gary Fulstetter, [FulstetterG@gmail.com](mailto:FulstetterG@gmail.com), 740-413-9012
- Clients will be notified a minimum of 24 hours in advance of any high impact testing
- If a stop test occurs, there will be an immediate notification sent out provided (Via Email + Phone)
- Stop testing conditions would be:
  - Client wants to halt testing
  - Any safety, legal, or regulatory risk
  - Discovery of sensitive data outside of the scope
  - Unintended service outage or degradation in performance

**Data Handling**

- Only collect necessary data, anyone who collected more data then required will be written up and reported
- All testing data and results will be collected and stored in a secure and encrypted repository that will only be accessed by the System Owner and the testers which all will be monitored
- Any sensitive customer and employee data included in the report will be redacted
- All the evidence collected will be retained for 30 days after final report has been released

**Reporting & Handoff**

- G&G Industries will provide one (1) comprehensive report at the end of this engagement which will include an executive summary
- As previously stated, the examination will go on for a full two weeks and operate within the stated hours
- The report deliverable will include:
  - The purpose of this engagement including the project's scope and approach
  - Positive security controls that were identified
  - Tactical recommendations to reduce the risk in the environment in the immediate term
  - Recommendations for preventing similar issues from recurring and for improving the client's overall security posture
  - Technical description and classification of each vulnerability
  - Vulnerability classifications that details the severity