# EasySec SOP (Standard Operating Procedure)

At EasySec, we aim to provide affordable and accessible cybersecurity to small banks and pharmacies across the state of Iowa. Through this, we aim to strengthen the security infrastructure of some of the most vulnerable small businesses and provide lasting and meaningful support to our customers.

## Purpose

> The purpose of this Standard Operating Procedure (SOP) is to provide clear and consistent guidelines for Working with Customer Environments.

## Scope

This SOP is applicable to:

- Employees of EasySec conducting Audits
- Employees of EasySec configuring devices within Customer Environments

This SOP covers the following aspects:

- Accounting
- Preservation of Client Environments

## Roles & Responsibilities

| Role | Responsibilities |
|---|---|
| Role 1<br>@Security Auditor | • Conduct Security Audits on Client Environment to determine weak spots, and points for improvement<br>• Suggest said changes to the client<br>• Inform and guide client on best security practices |

| | |
|---|---|
| Role 2<br>@System Administrator | • Deploy security appliances to Client's environment<br>• Configure said appliances for the Client<br>• Continually Manage tools such as SIEM/Firewall |

## Procedure

The following steps outline the procedure for Auditing and Securing Customer Environments with EasySec

### Step 1:

- Deploy our Linux Virtual Machine to test the security of the client environment.
- Document every step along the way, including making backups/snapshots of the client environment in the event that something we exploit it detrimental to business function.
- Conduct tests which will be repeated to a Tee, once security appliances are configured in order to gauge improvement.

### Step 2:

- Go over "Report Card" with client, showing them what they've done well, and what they've done poorly.
- Deploy Security Appliances, and configure them for the client's network.
- In the event of any damages, at this point, we would revert to the snapshot/backup that we had made.

### Step 3:

- Conduct a post-audit, displaying the changes that were made and what differences in security posture we had provided.
- Share with IT staff what we had done, including some concessions that they might have to make as a result of those changes.
- Training with IT and Customer Support Staff to prevent Phishing, and Social Engineering attacks.

## Resources

🔗https://docs.google.com/document/d/1MeZrIFmOh7k9yJtDmRdInP9gvVDg5pmE42NWSWueW-0/edit?usp=drive_link

## Review & Revision

👤 **SOP Owner:** @EasySec

🗳️ **Revision Request Form:** *Link Form*