# TAGITM InfoSec Program Startup Guide: First Things First

*"Amateurs hack systems, professionals hack people." – Bruce Schneier*

This guide should be helpful for anyone looking to develop or mature their cybersecurity program. We understand that every organization has different needs and is in a different stage of their cybersecurity journey. Many organizations haven't decided on which security framework to adopt and that's okay. These recommendations are relevant no matter which framework you choose.

1. **Interim Incident response plan** (contact list of all people to notify)
   a. This will be an interim plan for those that do not have anything in place. The objective is to have a base-line plan while you are working on the other items.
   b. For larger departments, identify who is responsible for what and what authority they have to execute actions without escalation, e.g., disable c-level accounts that are potentially compromised, shut off internet if a potential breach is detected. This is to empower your team in good faith so they can stop the bleeding instead of waiting for permission.
   c. Reach out to your emergency management team so you have state contact and potential resources in place if needed prior to an incident.
2. **Develop internal policies and procedures** (internal dept only)
   a. Have a procedure in place for documenting and hardening any device put on the network.
   b. Have a procedure in place for creating users with least privileges.
   c. Have a policy for granting external access to vendors with account expiration dates.
   d. Develop (start) Internal Business Continuity Plan. This may be part of the basic internal policies and procedures.
3. **Inventory Assets** (includes locations, network diagrams, hardware, software)
   a. Prioritize those assets by identifying what is public facing and storing sensitive data.
   b. Create a strategy to protect your assets, ensuring endpoint protection is installed where possible.
4. **Continuous Security Awareness Training**
   a. Start evangelizing basic security principles across your organization.
   b. Work towards a monthly cadence of awareness short training, focusing on single topics.
5. **Policies that are Org-wide** (Pick 3-5 to start with so you don't get overwhelmed)
   a. Incident Response Plan
   b. Change Control
   c. Acceptable Use
   d. Security patching
   e. Configuration Management - Standard technology deployment templates
6. **User your resources and build relationships**

**References**

1. **Interim Incident response plan**
   - a. NIST Special Publication 800-61 Rev. 2
   - b. The State of Texas Guide to Cybersecurity Incident Response
   - c. CIS Critical Security Control 17: Incident Response and Management (cisecurity.org)
2. **Develop internal policies**
   - a. See 5 below
3. **Inventory Assets**
   - a. IT Asset Management (nist.gov)
   - b. CIS Critical Security Control 1: Inventory and Control of Enterprise Assets (cisecurity.org)
4. **Continuous Security Awareness Training**
   - **a.** Statewide Cybersecurity Awareness Training | Texas Department of Information Resources
   - b. NIST Special Publication 800-50
5. **Policies that are Org wide**
   - a. Policy Template Guide - CIS Center for Internet Security
   - b. Information Security Policy Templates | SANS Institute
   - c. NIST Special Publication 800-18 Rev. 1
6. **User your resources and build relationships**
   - **a. TAGITM Cyber Security Resources**