Information Network Security Agency (INSA)

National Cyber Security Framework Development Methodology

Version 1.0

2014 EC

Information Network Security Agency (INSA)

National Cyber Security Framework Development Methodology

Version 1.0

2014 EC

Contents

Foreword

Information and communications technologies have become indispensable to the modern lifestyle. We depend on information and communications infrastructures in governing our societies, conducting business, and exercising our rights and freedoms as citizens. In the same way, nations have become dependent on their information and communications infrastructures and threats against its availability, integrity and confidentiality can affect the very functioning of our societies.

To help protect critical infrastructure, information and information system; INSA has published and is implementing a standard, "Critical Mass Cyber security Requirement Standard". This Cyber Security Frameworks (Policy, Procedure, Guideline and Plan) Development Methodology and Template document is prepared based on the Critical Mass Cyber Security Requirement Standard to help and guide organizations when developing their cyber security policies, procedure, guidelines and plans. This document is drafted by Cyber Security Standard Research and Development Team and revised by Cyber Security Governance and Management Division. It is expected yet to be reviewed by respective stakeholders. It should be amendable as a result of CMCSRS modification.

Draft national policies, laws, standards, and strategies that enable to ensure the information and computer-based key infrastructures security and oversight their enforcement upon approval is one of the power and duties are given to the Information Network Security Agency (INSA).

Therefore, this methodology is issued by Information Network Security Agency (INSA) pursuant to Article 13 of Information Network Security Agency Re-establishment proclamation Execution council of ministers Regulation No.320/2014.This document can be called as the first draft document of National Cyber Security Policy, Procedure, Guideline and Plan Development Methodology and Template.

Acronyms

Abbrevation	Decsription
CCSP	Corporate Cyber Security Policy
CIO	Chief Information Officer
CS	Cyber security
INSA	Information Network Security Agency
IS	Information Security
ISCSP	Issue Specific Cyber Security Policy
SSCSP:	System Specific Cyber Security policy

1. Introduction

Cyber security becomes a global phenomenon that knocks the door of every organization and nation. The truth is, we are connected to each other more than ever, and this creates a high vulnerability surface for the inside and outside attackers of the organizations/nation or any target. Most of the organization's businesses rely on sensitive information, critical infrastructures and information systems; if those critical/valuable information assets, infrastructures and information systems lack sufficient and efficient cyber security controls, they may lead into national and organizational instability. Placing different kinds of security control measures is not an option; it is a question of protecting/ensuring the national interest and business of organizations. Among many cyber security controls; administrative cyber security control is one, which helps to strengthen the organization's security capability.

Organization should place cyber security controls to protect their critical information, information systems and infrastructures. Security controls mainly classified as: administrative/procedural, technical/logical and physical controls. The administrative/procedural control highly relies on strategy, policy, procedure, guidelines, and plans.

To help protect the national and organizations' critical infrastructures, information and information systems, INSA, published and is implementing a standard "Critical Mass Cyber Security Requirement Standard". Among many requirements listed in the standard to ensure cyber security issues of the organizations is developing cyber security frameworks. Such as, cyber security policies, procedures, guidelines, strategies and plans, so organizations can develop and implement these frameworks as part of protecting their business. This document aims to help organizations' develop their own cyber security policies, procedures, guidelines, strategies and plans.

This document provides the means for the nation and organizations to develop the administrative cyber security controls to strengthen the overall cyber security status of the nation and organizations. Cyber security policies, procedure and guideline can be used as an active part of the national and organizational effort to protect their critical/valuable information assets.

This cyber security framework development methodology and template document serves as a guiding document for policy developers, it includes the minimum information/component required to be included in a cyber security policy, procedure, guidelines, plan and it has a template.

Policy is a formal, brief, and high-level statement that embraces an organization's general beliefs, goals, objectives, and acceptable procedures for a specified subject area. Policies always state required actions, and may include pointers to standards. Policies can be considered the "constitution" of security governance and must be clearly aligned with the strategic security objectives of the organization.

There are **three** types of cyber security policy addresses in this document:

Corporate cyber security policy is a foundational policy designed to provide direction for the organization's entire security effort and the rest of the organization's cyber security frameworks will be created under its guidance.

Issue specific cyber security policy are shaped to cover cyber security issues, and address issues of current relevance and concern to the organization and provide instruction for employees to follow regarding the proper usage of cyber security.

System specific cyber security policy it is often functions as standards or procedures to be used when configuring and maintaining systems. It is much more focused, since it addresses only one specific system.

This document also addresses cyber security procedures, guidelines and plans. **Procedures** describe the processes. That is, who does which duties and responsibilities when under what criteria pr conditions? **Guideline** is general statement, recommendations, or administrative instructions designed to achieve the policy's objectives by providing a framework within which to implement procedures. **Plan** is aimed at achieving specific goals or objectives within a specific timeframe. It explains in detail what needs to be done, when, how and by whom.

Organizations should follow and refer this document when developing the organizational cyber security policies, procedures, guidelines, and plans.

2. Objective

2.1. General Objective

The general objective of this document is to provide organizations and cyber security policy makers' comprehensive methodologies and templates on cyber security policies, procedures, guidelines and plans.

2.2. Specific Objective

A. To simplify organizations' effort while developing their own cyber security strategies, policies, procedures, guidelines and plans.
B. Serves as a guiding document for effective cyber security policy, procedure, guideline and plan preparation and development.
C. To lay a pavement for organizations' cyber security policies, procedures, guidelines and plans developers.

3. Scope

This document covers cyber security frameworks; policies, procedures, guidelines, and plans which are applicable in organizations regardless of their size, complexity and business nature.

4. Purpose

The purpose of this cyber security policy, procedure, guideline and plan development methodology and template is to help and guide organizations in implementing Critical Mass Cyber Security Requirement Standard and when developing their own cyber security frameworks.

5. Principles

These are some of the principles organization should firmly consider when they develop cyber security policies, procedures, guidelines, and plans.

- Risk Based
- Contextualize
- Cost effective
- Tipping Point
- Alignment

Note: Other principles of the organization can be used as long as those organizational principles do not contradict with the above principles. For further description of the principles refer the Annex.

6. Corporate Cyber Security Policy

6.1. Overview

Corporate cyber security policy, which is also known as Security Program Policy (SPP) is a general purpose security policy. Corporate cyber security policy supports the mission, vision and direction of the organization. It is a high level corporate policy which defines the purpose of the cyber security programs and it sets strategic directions, scope, & tone for organization's security efforts, assigns responsibilities for various areas of security programs, guides development, implementation, and management requirements of security program, resources for its implementation and overview of corporate philosophy on security. Usually, it is drafted by top leader or CIO of the organization. It is a foundation for **issue specific** and **system specific** cyber security policies.

Basic rules to follow when shaping policy; the policy should

- Never conflict with law
- Be designed in a way it properly supported and administered security issues
- Contribute to the success of the organization
- Involve end users of information systems

6.2. Methodology

This sections show the minimum requirements/components to be considered when developing corporate Cyber Security Policy, but not limited to:

Introduction

Brief explanation on the subjects of the entire cyber security policy program of the organization, and overall of security program, issues regarding corporate cyber policy of organization should address or cover, while emphasizing on the current status organization and its security situation. It also describes the goal of security programs and in which the security programs support mission, vision and direction of the organization. This section should also incorporate the organizational corporate policy intended result when the organization complies with its cyber security policy.

Objective

Describe the objective of this corporate cyber security policy in a way to show how it can support the overall missions of organization. Determines general and specific objective of security program

aims to achieve within a time frame and with available resources. The objective can be subsequent result of the development and implementation the security program that organization wants to achieve or the significance of the program in the achievement of organizational mission and vision.

Scope

The scope of the corporate cyber security policy may be seen from two directions; one from boundary of applicability in order to define where, when, how and to whom the policy should be applied. The other is from the view of which security program should be covered in the policy.

Policy Statement

Policy statement provides a brief explanation or rationale of the policy, what the policy hopes to accomplish and include how the policy is related to the organization's core mission and values. This policy statement provides specific direction for the intended audience. These are some of the questions answered through the policy statement, but not limited to;

- Who is the primary audience? (Who needs to follow the policy?)
- In what situation(s) does this policy not apply?
- What are the major conditions or restrictions?
- What is expected of the employee?
- Are there exclusions or special situations?

Responsibilities

Describes who is responsible for actions to meet the requirements of the Corporate Cyber Security Policy. And who is responsible for each entire security program and assigns the appropriate responsibilities to parties from varies part of organization to accomplish the security program. It can assign responsible bodies to each role of the program based on National Cyber Security Career Path.

Related Document

In this section, other policies, procedures, forms, guideline and other resources relevant to the achievement of the objectives will be mentioned and/or discussed, usually, by providing additional details concerning security program. It also draws a picture about how the Corporate Cyber Security Policy is aligned with other related documents/resources.

Policy Compliance

a. Compliance Measurement

To measure the policy compliance organization should select policy compliance measurement mechanisms and methods including, but not limited to business tool reports, internal and external audits, and feedback.

b. Exceptions

Organization should define a responsible body for granting any exception to the policy.

c. Non-compliance

Describe the list of possible sanctions if a user (employee) violates a policy or includes a general statement like: "Any user who violated this policy is subject to disciplinary action up to and including termination of employment, including criminal prosecution and Punishment with law of state.

Contact Information

Details of who should be contacted in connection with policy. A group or mailbox rather than an individual is preferable here as these are less likely to change.

Definitions/Glossary

This section contains a list of key words and phrases, thus words or phrases with meanings unique to the security program and uncommon words. It recommends be define and list in alphabetical order, words or phrases which may not be familiar to, or might be misunderstood or interpreted the concept of program, definition help reader guide.

Revision History

The policy owner is responsible for review, update and change of Corporate Cyber Security Policy. But the change is not expected to be frequent. Yet, whenever there is a strategic change. When the policy revised state the reason why the policy is revised, when, who made the change and other related information.

Version	Description	Revision Date	Review Date	Reviewer/Approver Name
1.0	Initial Version			

6.3. Corporate Cyber Security Policy Template

Cover Letter:

Title: "Title of the Corporate Policy"

Document reference number	
Revision number	
Approval date	
Revision date	
Document developed by	
Document approved by	
Responsibility for implementation	
Responsibility for revision and audit	

Document reference number:

Assign the reference number of the corporate policy.

Revision number:

Assign a number each time the document is revised.

Approval date:

Date when the corporate policy has been approved

Revision date:

Date the corporate policy is due for revision

Document developed by:

This should be the name of chair of the development group. The members of the working group should be listed as an appendix.

Document approved by:

This is the name of the Chair of the Board or Core Management Committee who has final sign off.

Responsibility for Implementation:

Identify and name the individual who is responsible for rolling out the implementation of the corporate policy. This individual's job title should also be documented.

Responsibility for revision and audit:

Identify and name the individual/organizational entity with responsibility for revision and audit. This individual's job title should also be documented.

Tip: Besides, a cover letter from the president of the board of directors introduces the corporate policy. It gives the corporate policy a stamp of approval and demonstrates that the organization has achieved a critical level of internal agreement.

Introduction:

The corporate cyber security policy's Introduction section states the types and levels of security over the organization critical information, information system, guides the development, implementation, and management requirements of the cyber security program and infrastructure, and how it helps to achieve the organization mission. The cyber security stance of the organization will be stated here.

This section describe the strategic direction, scope, and tone for all security efforts, expresses the security philosophy within cyber environment, and states how it supports the mission, vision, and direction of the organization. In addition, this section includes the reason or rationale for the corporate cyber security policy, may describe the problem or conflict that the policy will resolve and may include reference to regulatory or legal reasons for the making of the policy. In one to two pages, this section summarizes the corporate policy.

Objective:

Specifies why the corporate cyber security policy is needed and stipulates the intent of the policy. Hence, deliver adequate facts about the objectives and purpose of the corporate policy, and also bring the audience a brief image of what corporate cyber security will state and why it is needed.

Scope:

Organization should lays out exactly what the corporate policy covers. Precisely what issues, organizational unit or technological system that the corporate cyber security policy covers.

Policy statement:

Roles	Responsibilities

Top management (Executives)	• Accountable and responsible for leading and directing the corporate organization • Highest organizational leader and sets strategic direction, policies • Approves corporate cyber security policy
Chief cyber security Officer	• Accountable for all aspects of the Organization's cyber security. • Drafts corporate cyber security policy
Cyber security officers	• Responsible for the security of the IT infrastructure. • Plans against security threats, vulnerabilities, and risks. • Implement and maintain Security Policy documents. • Ensure security training programs. • Ensure IT infrastructure supports Security Policies.
Information Owners	• Help with the security requirements for their specific area. • Determine the privileges and access rights to the resources within their areas.
Cyber security Team	• Implements and operates cyber security. • Implements the privileges and access rights to the resources. • Supports Security Policies.
Users	• Meet Security Policies. • Report any attempted security breaches.

The corporate policy should be directly traceable to strategy elements. It should be apparent that a policy that contradicts the strategy is counterproductive. So that corporate policy should be consistent with and support the intent and direction of the strategy. For example, if the objective is to become CMCSRS compliant over a five year period, then the strategy must consider which elements are to be addressed first, what resources are allocated, how the elements of the standard can be accomplished and so forth while each of the relevant five (5) capabilities building and thirty-two (32) main processes focus areas should be the subjects of a corporate policy. In practice, this can be effectively accomplished with about many specific policies (either issue specific or

system specific policies) for even large organizations. Each of the corporate policies is likely to have a number of supporting 'issue specific' and 'system specific' policies or standards typically based on their security areas.

Hence, this section states about the corporate policy and indicates issues specific and system specific policies barely as indicators. The policy statement supposed to describe what the Corporate Cyber Security Policy hopes to accomplish and include how the policy is related to the organization's core mission and values. Policy statement should include the principles of the Corporate Cyber Security Policy: what is permitted or prohibited, what is required, or how issues will be handled.

Roles and Responsibilities:

Clearly define the appropriate personnel/organizational entity to fulfill the roles and responsibilities in a description of who is responsible for which elements of the security of the system or issue being covered. This is important to enforce accountability. Corporate Cyber Security Policy identifies all the roles involved and lists their specific responsibilities of each recognizable user, including management, employees and residual parties. Defines the organizational structure designed to support cyber security within the organization.

Policy Compliance:

This section states what is considered a violation and the penalties for non-compliance. The violation of a policy usually implies an adverse action which needs to be enforced.

Relevant Documents:

This section provides all relevant and referenced documents in the process of cyber security corporate policy development. Consider what other documents; regulations, proclamation used to provide additional or further details about the "title of cyber security corporate policy". This section also outlines lists of other standards, legislation, policies, strategies that influence and are influenced by this corporate cyber security policy document.

Appendices:

Additional information is included in this section that will support and provide a rationale for the corporate policy. Besides, this section may include explanation of key technical terms those are

referred to in the corporate policy and lists of references used in the development. Also, List the major outcomes which are expecting from developing and implementing corporate cyber security policy. This may described by diagrams, flow charts or models. Each appendix recommends to be incrementally numbered using roman numerical script (e.g. Appendix I, II, III, and IV etc.).

7. Issue Specific Cyber Security Policy

7.1 Overview

An Issue-Specific Policy is intended to address specific needs within an organization. Issue-specific policies are developed to focus on areas of current relevance and concern to an organization. Issue-specific policies may also be appropriate when new issues arise, such as when implementing a recently passed law requiring additional protection of particular information. Program policy is usually broad enough that it does not require much modification over time, whereas issue- specific policies are likely to require more frequent revision as changes in technology and related factors take place. In general, for issue-specific, the issuer is a senior official; the more global, controversial, or resource-intensive, the more senior the issuer.

There are three common approaches to implementing ISCSP. They are: Independent ISCSP documents, each tailored to a specific issue. A single comprehensive ISSP document covers all issues. A modular ISCSP document unifies policy creation and administration while maintaining each specific issue's requirements.

7.2 Focus areas of ISCSP

These are the issues organization ISCSP should highly consider, but not limited to;

- **Personnel security policy:** a policy which applies to new employees, re-hired employees, transferred, or promoted employees, as well as third parties such as temporary staff, contractors, and consultants who have relation with human resource management in the organization.
- **Acceptable use policy (AUP):** is a set of rules applied by the organization or administrator of a network, website, data/information, device or service, that restrict the ways in which the network, website, data/information, device or system may be used and sets guidelines as to how it should be used;
- **Information classification policy**: It sets out the requirement to define classes of information handled by the organization;
- **Change management policy**: increase awareness and understanding of proposed changes across an organization and ensure that all changes are made in a thoughtful way that minimize negative impact to services and customers;

- **Hardware and software procurement/acquisition, development and maintenance policy**: hardware and software products are reviewed, purchased and maintained, with respect to data security, operational integrity, and long-term sustainability;
- **Password policy**: set of rules designed to enhance computing device security by encouraging users to employ strong passwords and use them properly;
- **Internet usage policy:** provides employees with rules and guidelines about the appropriate use of company equipment, network and Internet access.

There are other issues the organization ISCSP may incorporate considering their context, but not limited to;

- **Use of Electronic mail policy**: is to ensure the proper use of email system and make users aware of what considers as acceptable and unacceptable use of its email system;
- **Network security policy**: lays out some of the basic architecture of the company security/network security environment;
- **Asset Management policy**: All Assets are documented and identifiable throughout the entire asset lifecycle;
- **Access control management policy**: ensure the organization has adequate controls to restrict access even remotely to systems, data and internal network;
- **Physical and environmental security policy**: defines the requirements for protecting organization Cyber security resources from physical and environmental threats in order to reduce the risk of loss, theft, damage, or unauthorized access to those resources;
- **Malicious software protection policy**: only allowing the software installation in the organization network and computing device from recommended site;
- **Encryption policy**: ensure that organization communication and computing device may be used to store or access sensitive data;
- **Risk assessment policy:** empower Information security to perform periodic information security risk assessments for the purpose of determining areas of vulnerability, and to initiate appropriate remediation;
- **Back up, restoration/recovery, removing, disposal of data/computer, and disaster recovery policy**: Include confidentiality (in handling, storage and transmission), integrity

(e.g. validation processes), availability (e.g. backups), recovering, removing and disposal of data and computers;

- **Data center security policy**: ensure that the data center, and the equipment hosted therein, remains secure by having in place a policy and procedures to restrict access to the data center to authorized persons;
- **Incident management policy**: ensure that any incidents that affect the daily operations of the organization cyber space (environment) are managed through an established process;
- **Antivirus policy**: help to prevent infection and protect user applications, data, files, and hardware of organization computing device, networks, and technology systems from malware;

7.3 Methodology

To prepare ISCSP document these are the minimum requirement/component incorporated while developing, but not limited to;

i. **Introduction**

This section is brief explanation on the subjects of the issue of the Issue Specific Policy, and overall situation about specific point on cyber security, regarding issues that address corporate cyber security policy of organization, while emphasizing on the current status of organization on the issue. This section also describes the goals of the Issue Specific Policy and/or describes the consequential intended result if the organization complies with to its issue specific cyber security policy.

ii. **Objectives**

Determine the general and specific objectives Issue Specific Cyber Security Policy. The objective of Issue Specific Cyber Security Policy is to show how it can support both security programs/Corporate Cyber Security Policy and the overall missions of the organization; the objective of Issue Specific Cyber Security Policy is the subsequent result of the development and implementation of the issue specific policy. That is, significance of Issue Specific Cyber Security Policy to Corporate Cyber Security Policy of the organization.

iii. **Scope**

Determining scope of the Issue Specific Cyber Security Policy may be seen from two directions one from boundary of applicability in order to define where, when, how and to whom the policy should be applied. The other is from the view of which issue and activities should be cover on the policy.

iv. **Policy Statement (issue statement)**

Provide a brief explanation or rationale of the issue specific cyber security policy, what the ISCSP hopes to accomplish and include how the ISCSP is related to the organization's core mission and values, accomplish and alignment with Corporate Cyber Security Policy. The organization's position on the issue will need to be clearly stated and defined.

This ISCSP statement provides specific direction for the intended audience. These are some of the questions answered through the policy statement, but not limited to;

- Who is the primary audience? (Who needs to follow the policy?)
- In what situation(s) does this policy apply?
- What are the major conditions or restrictions?
- What is expected from the ISCSP?
- Addressed of ISCSP
- Impact of ISCSP
- Role of ISCSP

v. **Current Situation of issue**

Clearly and concisely present the current situation with any contributing history, and any trends, cycles, changes or future developments that are relevant to the issue. Describe what are the situations of the organization regarded with the issue, and case or event that drive to issue based on overall situation of Corporate Cyber Security Policy.

vi. **Key Issues**

Clearly define the most important issues as they relate to the current situation and the overall purpose of this issue and the organization mission. Key issues are usually those strengths, weaknesses, opportunities, threats, capability gaps and impediments that impact issue on business performance the organization.

vii. **Action**

Describe statements of specific actions or activities that will be done to achieve a goal the issue within the constraints of the objective. Define actions required to achieve the goal of Issue Specific Cyber Security Policy within defined set of timeframe, each of actions of the ISCSP and supportive action relevant to issue. That is, action plan(s), which consider the required resources for the implementation of the Issue Specific Cyber Security Policy. Such as, budget, human power, physical resource…

viii. **Roles and Responsibilities**

Describe who is responsible for specific actions to meet the requirements of the policy, Issue Specific Cyber Security Policy. Assign responsible body to each role of issue based on National Cyber Security Career Path and the required relevant security clearance and briefings for that specific action.

Responsible	The department or person(s) responsible for developing and implementing the Issue Specific Cyber Security Policy.	**The Cyber Security Department,**
Accountable	The person who has ultimate accountability and authority for the specific Issue Specific Cyber Security Policy.	**Data owner**
Consulted	The person(s) or groups to be consulted prior to final Issue Specific Cyber Security Policy implementation or amendment.	**Cyber security steering committee, Senior management,**
Informed	The person(s) or groups to be informed after Issue Specific Cyber Security Policy implementation or amendment.	**employees, contractors …… and other relevant or interested parties**

ix. **Key outcomes**

Describe the business outcomes if the objectives, mentioned on objective section are met.

x. **Key Performance Measures and Targets**

Establish key performance measures/indicators, performance targets and time lines of action plan of the issue to improve performance, to achieve the objectives, mentioned on objective section. Performance Measures parameters can be the required time, expected or targeted goal and cost… performance should be continuously evaluated and improved based on stated measures of performance. It is a measurable value that demonstrates how effectively the organization is achieving key Issue Specific Cyber Security Policy objectives. Organizations use key performance indicators at multiple levels to evaluate their success at reaching targets.

xi. **Points of Contact**

Regarding Issue Specific Cyber Security Policy, the organization should assign a right person to give further information, clarity, and guidance. Though, all employees are responsible regarding cyber security issues of the organization, yet assign specific as a point of contact.

xii. **Definition**

Here, list all key words and phrases with their meanings, which are unique to the Issue Specific Cyber Security Policy and are uncommon words to the organization's context. It recommended list and define the key words and phrases in alphabetical order.

xiii. **Policy Compliance**

a. Compliance Measurement

To measure the policy compliance, organization should select policy compliance measurement mechanisms and methods including, but not limited to business tool reports, internal and external audits, and feedback.

b. Exceptions

Organization should define a responsible body for granting any exception to the policy.

c. Non-compliance

An employee found violating this policy may be subject to disciplinary actions, minor administrative disciplinary measures, termination of employment, and/or punishment with law of state.

Describe the list of possible sanctions if a user violates the policy or include a general statement like: "Any user who violated this policy is subject to disciplinary action up to and including dismissal, including criminal prosecution".

xiv. **Related documents**

Describe other policies, procedures, forms, guideline and other resources relevant to the achievement of the objectives of Issue Specific Cyber Security Policy. Usually, such frameworks provide details about the concerning issue, and draw a picture of alignment of Issue Specific Cyber Security Policy with other related documents/frameworks. Examples may include other policies, Acts of Parliament (or sections of relevant text).

xv. **Review and Revision**

The policy owner is responsible for frequent review, update and change. Whenever there is a strategic change and when there is change on the organizational Corporate Cyber Security Policy and Issue Specific Cyber Security Policy requires alignment with the corporate cyber security policy. When the policy is revised, state the reason why the policy is revised, when, who made the change and other related information.

Date of creation/change	**Responsible**	**Summary of creation/change**
Click or tap to enter a date.		

7.4 Issue Specific Cyber Security Policy Template

Cover Letter:

Title: "title of issue specific Cyber security policy"

Document reference number	
Revision number	

Approval date	
Revision date	
Document developed by	
Document approved by	
Responsibility for implementation	
Responsibility for revision and audit	

Document reference number:

Assign the reference number of the corporate policy.

Revision number:

Assign a number each time the document is revised.

Approval date:

Date when the issue specific Cyber security policy has been approved

Revision date:

Date the issue specific Cyber security policy is due for revision

Document developed by:

This should be the name of chair of the development group. The members of the working group should be listed as an appendix.

Document approved by:

This is the name of the Chair of the Board or Core Management Committee who has final sign off.

Responsibility for Implementation:

Identify and name the individual who is responsible for rolling out the implementation of the issue specific Cyber security policy. This individual's job title should also be documented.

Responsibility for revision and audit:

Identify and name the individual/organizational entity with responsibility for revision and audit. This individual's job title should also be documented.

Overview:

Provide background information on the issue that the policy will address and states the types and levels of security over the information technology (cyber) resources and capabilities that must be established and operated in order for those items to be considered secure.

Objective:

Specifies why the policy is needed and the intention of Issue Specific Cyber Security Policy, and provide enough information about the objectives and purpose of issue specific policy, and also deliver the audience a brief picture of what the "title, Issue Specific Cyber Security Policy" will state and why it is needed.

Scope:

Lays out exactly who and what the policy covers; employee/staff, contractors, interested parties, information system, organization boundary etc. who this policy applies to, and who is affected by the issue specific Cyber security policy or needs to read it.

Policy Statement:

This section provides statements on each aspect of the policy. What you actually want to say about the issue, and where an organization explain and describe about the issue specific Cyber security policy and what it really means for the organization or organization position on the issue. The policy statement supposed to describe what the issue specific Cyber security policy hopes to accomplish and include how the policy is related to the organization's core mission and values. Issus specific cyber security policy statement includes what is permitted or prohibited, what is required, or how issues will be handled.

Current Situation of issue

Describe the current situation regarding to issue with respective of corporate cyber security policy and organizational mission, align with issue.

Key Issues

Clearly define the most important issues as they relate to the current situation for this Section, and the overall purpose of this issue and the companies mission. Key issues are usually those strengths, weaknesses, opportunities, threats, capability gaps and impediments that impact on business performance

Action

Describe statements of specific actions or activities that will be used to achieve a goal within the constraints of the objective.

Responsibilities:

It is important that the issue specific Cyber security policy detail the specific responsibilities of each identifiable user population, including management, employees and residual parties. Identify all the roles involved and their responsibilities in the enforcement of the policies (enforcement of accountability).

Roles	**Responsibilities**
Chief Cyber security Officer	• Accountable for all aspects of the Organization's cyber security.
Cyber security officer	• Responsible for the security of the IT infrastructure. • Plan against security threats, vulnerabilities, and risks. • Implement and maintain Security Policy documents. • Ensure security training programs. • Ensure IT infrastructure supports Security Policies.
Information Owners	• Help with the security requirements for their specific area. • Determine the privileges and access rights to the resources within their areas.
Cyber security Team	• Implements and operates Cyber security. • Implements the privileges and access rights to the resources. • Supports Security Policies.
Users	• Meet Security Policies. • Report any attempted security breaches.

Related documents

Lists all references mentioned in the issue specific Cyber security policy including organizational procedures, standards, government code (legislation), guidelines, and forms uses to provide additional or further details about the "title of issue specific Cyber security policy".

Key outcomes:

List the major outcomes which are expected from developing and implementing "title of issue specific Cyber security policy".

Key Performance Measures and Targets

Defines key performance measures/indicators, performance targets and time lines in conjunction with the strategies to assess and improve performance.

Point of contact

This section is about assigning a responsible person who assists an end user who has difficulties to understand or to implement "title of issue specific Cyber security policy". Further information and advice on this issue specific cyber security policy can be obtained from [Insert name, email and telephone number of appropriate employee].

Definition

Define meaning of key or unique terms used in the issue specific Cyber security policy which may not be familiar to, or might be misunderstood by a reader. For clarity, any technical terms should be defined.

Policy Compliance:

This section states what is considered a violation and the penalties for non-compliance. The violation of a policy usually implies an adverse action which needs to be enforced.

Review and Revision

This section states the author and owner of the policy. It also describes the conditions and process in which the policy reviewed. And this part of issue specific cyber security policy is aimed to check the life span of a specific version of the whole document. In case separate into several issue specific cyber security policy documents, ensure there is a version history for each one of them. Issue specific cyber security must be reviewed and eventually updated periodically to keep up with changes in risks, technologies and regulations.

Version	Description	From	To	Responsible/ Author	Summary of change
	Initial version	Click or tap to enter a date.	Click or tap to enter a date.		

8. System Specific Cyber Security Policy (SSCSP)

8.1. Overview

Focus area of corporate and issue specific policies that you review in the above sections of this document are very broad; whereas the focus area of SSCSP is very specific and applied at a particular system level.

A System-specific policy is a policy written for a specific system or device. This type of policy in general is more specific, technical and more focused on nature of specific system, and is particularly developed to safeguard specific system from various threats. In certain situations, SSCSP has a look of step by step guiding document like standard or a procedure to carry out some sort of task that is done on a particular system, when configuring, maintaining and operating a system.

The most important reason for the need of SSCSP is to realize the high level security objectives stated in corporate and issue specific policies of the organization by applying a more focused and specific rule for each system.

Several SSCSP policies of an organization can be organized in a single system policy document. For instance, an organization may develop a policy for each boundary firewall in its segregated network and for several core business systems run in its datacenter. All of these policies can be published as single large system specific security policy of the organization. If it is not manageable, organizations can have different documents for each of the policies.

8.2 Focus Area

Organizations can develop a SSCSP for the following technologies based on the organizational business requirements, but not limited to.

- Routers and switches
- Intrusion detection and prevention systems
- Different firewalls
- Core business applications
- Different servers
- Storage Technology
- Wireless routers and Access points

8.3 Methodology

Here are the components a SSCSP should have, but not limited to:

i. Introduction

This section is a brief explanation of the subjects of the policy and the context of the publication. It also describes the overall objectives, functions, or tasks that the policy is designed to accomplish and the circumstances under which the policy should be used. To describe the overview of the policy organization can refer their mission and vision, other internal documents, national and international policy, like, Critical Mass Cyber security Requirement Standard that is issue by INSA.

ii. Purpose

Since it is more system focused policy, the organization should plainly put the main purpose of the policy in a way to show how it can support both security programs and the overall missions of organization. The purpose of system specific cyber security policies should address regulatory constraints, protection of highly sensitive data and the safe use of specified system. To write the purpose organization can refer their mission and vision, purpose of other policy, procedure, guideline or protocol, purpose of Critical Mass Cyber security Requirement Standard.

iii. Scope

The scope of the policy may be seen from two directions one from boundary of applicability in order to define where, when, how and to whom the policy should be applied. The other is from the view of which system and what type of activities should be done on the systems. Therefore, it is more important to describe boundaries of the policy from various points of view. To describe the scope of the system specific cyber security consider the scope of your organization, identify user of your organization internal and external, see the organization's cyber security strategy and policy, identify is this policy is applies to all of the user or to some of them.

iv. Policy Statement

SSCSP policy statements should comprise more general security objectives from Corporate Cyber Security Policy and detail technical requirements acquired for each security objectives from Issue

Specific Cyber Security Policies of the organization. These are the more general or high level security objectives defined by the high level organizational security policy and issues specific cyber security policies order to keep the alignment of the security from the top to bottom. Therefore, SSCSP should comprehensively include points used to attain high level security objectives defined by different policies of the organization.

SSCSP should address potential security issues of the system during.

- Procurement of the systems
- Installation of the systems
- Configuration of systems
- Deployment of systems
- Operation of systems
- Maintenance of systems
- Disposal or destruction of the system

SSCSP should address the following issues of systems but not limited to

- Configuration requirements of the system
- Access control requirements of the system
- Testing issues of the system
- System log management
- Supporting components of the system
- System related contingency plans
- System connection types
- Backup and recovery issues of the system
- Location and physical access of the system
- Functional and nonfunctional services of the system
- Changes on the system
- Configuration requirement
- Monitoring requirement
- Patch management of the system

v. Responsibility

Identifies who is responsible for adhering to, implementing, and monitoring relevant aspects of the policy. To assign the responsibility organization can refer job description of departments, units, offices individual employees, also refer Critical Mass Cyber Security Requirement Standard.

vi. Policy compliance:

Compliance measurements: policy compliance measurement mechanisms and methods should be clearly stated.

Exceptions: it is important to define how and by whom exceptions should be managed.

Non–compliance: including the disciplinary or other types of penalty measurement for non-compliance of SSISP, is essential to ensure the commitment of employees and business unites to comply with the policy proactively.

vii. Related document

List of related policies, procedures, standard and guidelines should be included in order to create an alignment with other policies and standards. It also, identifies any other documents that are relevant or important to the policy. While all written material within the organization is related in one way or another, there will often be particular documents that should be read in conjunction with the policy.

viii. Revision history

When the SSCSP policy revised defines who is responsible for making updates and revisions to the policy and how often these will take place. It may be useful to include a reference to the document as a "living document" which can be updated as determined by those responsible for updates and revisions. This will ensure that any ad hoc revisions are accounted for as well as scheduled updates. Information should also be included detailing where the policy will be published and how employees can access it.

8.4 System Specific Cyber Security Policy Template

Cover letter:

Title: "title of system specific cyber security policy".

Document reference number	
Revision number	
Approval date	
Revision date	
Document developed by	
Document approved by	
Responsibility for implementation	
Responsibility for revision and audit	

Document reference number:

Assign the reference number of the policy.

Revision number:

Assign a number each time the document is revised.

Approval date:

Date when the policy has been approved

Revision date:

Date the policy is due for revision

Document developed by:

This should be the name of chair of the development group. The members of the working group should be listed as an appendix.

Document approved by:

This is the name of the Chair of the Core Management Committee who has final sign off.

Responsibility for Implementation:

Identify and name the individual who is responsible for rolling out the implementation of the policy. This individual's job title should also be documented.

Responsibility for revision and audit:

Identify and name the person(s) with responsibility for revision and audit. This individual's job title should also be documented.

Introduction

Provide background information on the system specific that the policy will address and states the types and levels of security over the cyber security resources and capabilities that must be established and operated in order for those items to be considered secure.

Purpose:

Specifies why the policy is needed and the intention of the system specific cyber security policy, and provide enough information about the purpose of system specific policy, and also deliver the audience a brief picture of what "title of system specific cyber security policy" will state and why it is needed. It should describe how to address regulatory constraints, protection of highly sensitive data and safe use of specific system.

Scope:

This section lays out exactly who and what the policy covers; employee/staff, contractors, interested parties, information system, organization boundary, etc. who this policy applies to, and who is affected by the system specific cyber security policy or needs to read it.

Policy Statement:

This section provides statements on each aspect of the policy. What you actually want to say about the system, and where an organization explain and describe about the system specific cyber security policy and what it really means for the organization or organization position on the system. The policy statement supposed to describe what the system specific cyber security policy hopes to accomplish and include how the policy is related to the organization's core mission and values. System specific cyber security policy statement includes what is permitted or prohibited, what is required, or how system will be handled.

Policy Compliance:

This section states what is considered a violation and the penalties for non-compliance. The violation of a policy usually implies an adverse action which needs to be enforced. The compliance measurement mechanisms and methods should be clearly stated and if there are exceptions it should define how and by whom the exceptions are managed.

Related documents:

Lists all related documents to the system specific cyber security policy including organizational procedures, standards, government code (legislation), guidelines, policy and forms uses to provide additional or further details about the "title of system specific cyber security policy".

Revision history:

This section of the system specific cyber security policy is aimed to check the life time of a specific version of the whole document. In case you separate into several policy documents, ensure there is a version history for each one of them. System specific cyber security policy must be reviewed and eventually updated periodically to keep up with changes in risks, technologies and regulations.

Version	Description	From	to	Responsible/ Author	Summary of Revision
1.0	Initial version	Click or tap to enter a date.	Click or tap to enter a date.		

9. Procedure

9.1 Overview

One of the administrative (managerial) controlling mechanisms of cyber security is establishing a cyber security policy, and to implement the policy effectively a procedure is a key factor. This procedure development methodology shows organization's framework (specifically, procedure) developer the method on how to develop a procedure. Having a procedure increases the performance of the task, creates a consistent working environment and effective procedure reduces or eliminates mistakes.

Generally, procedures are a step by step instruction to accomplish a given task and detailed steps required to perform an activity within a processes. Procedures are the responsibility of operations, including security operations. Procedures must be unambiguous and include all necessary steps to accomplish specific tasks. They must define expected outcomes, displays and required conditions precedent to execution. Procedure must also contain the steps required when unexpected results occur.

9.2 Steps to Develop Procedure

Procedures emanate from processes and policies. Therefore, identifying, understanding and documenting the processes and policy are the founding points to develop a procedure. In the processes, answer explicitly what is the objective of the processes, gather detail information on the processes which you are making into a procedure.

Once identifying the processes and policy, the next step is which processes and policy need a procedure. Processes and policy should have procedures, but doesn't mean all processes and policy should have procedures. Consider the following issues, but not limited to will tell the need for making of a procedure for certain process (considering the organization context is very important).

- When a processes is complex, lengthy, and routine (but everyone should seriously follow rules);
- When a processes demands consistency and involves documentation;
- When a processes involves significant and has serious consequences if done wrong;

9.3 Focus Areas

Focus areas to establish a procedure, but not limited to;

- **Personnel security procedure:** a procedure which applies to new employees, re-hired employees, transferred, or promoted employees, as well as third parties such as temporary staff, contractors and consultants;
- **Incident response report procedure:** is a procedures aimed at identifying, investigating and responding to potential security incidents in a way that minimizes impact and supports rapid recovery;
- **Information (Security) classification procedure:** enhance the confidentiality, integrity and availability of Information Assets and Information Systems;
- **Backup and recovery procedure:** is a method which is essential for data protection and security;
- **Change management procedure:** is about establishing a procedure for proposed changes across an organization to create awareness and understanding;
- **Supply chain relationship management procedures:** It guide the relationship between the supply and chain management;
- **Physical security procedure:** Shows how to handle the physical security of the organization;
- **System accreditation procedures:** assuring the technical competence and management system;
- **Internal security audit procedure:** can keep compliance programs on track;
- **Password procedure:** a procedure a user strictly follows changing the password;
- **Vulnerability assessment procedure:** uses as a proactive step to secure the organization infrastructure;
- **Hardware and software procurement/acquisition development and maintenance procedure:** Enable the hardware, software procurement/acquisition development and maintenance follows a strict process to ensure data security, operational integrity, and long-term sustainability;

9.4 Methodology

Here are some of the requirements/components consider while developing a procedure, but not limited to;

i. **Introduction**

This section is a brief explanation of the subjects of the procedure and the context of the publication. Describes the overall objectives, functions, or tasks that the procedure is designed to accomplish and the circumstances under which the procedure should be used. To describe the overview of the procedure organization can refer their mission and vision, other internal documents, national and international procedures, like Critical Mass Cyber security Requirement Standard that is issue by INSA.

ii. **Objective**

State the main objective of the procedure; this will explain the reason for the procedure and will help readers understand how the procedure should be used. The objective of the procedure should be to achieve the mission and vision of the organization should be included. To write the objective organization can refer their mission and vision, objective of other policy, procedure, guideline or protocol, objectives of Critical Mass Cyber security Requirement Standard.

iii. **Scope**

The scope of this procedure may see in two directions, the first one to whom this procedure applies and the second one is what this procedures covers. Describe the procedure indicating who and what is covered by the procedure. Also, if applicable, the scope also lists the other procedures managed by this procedure. To describe the scope of the procedure consider the scope of your organization, identify user of your organization internal and external, see the organization's cyber security strategy and policy, identify is this procedure is applies to all of the user or to some of them.

iv. **Roles and Responsibilities**

In this section, lists departments, units, offices, and individual job titles for those who have responsibility for aspects of daily control and coordination of the procedure, authority to approve exceptions to the procedure (if applicable), and procedural implementation (including responsibility for any required electronic or written forms). To assign the role and responsibility

organization can refer job description of departments, units, offices individual employees, refer also Critical Mass Cyber security Requirement Standard this standard indicates what should individual and managements do to secure their critical information and information system. The following table is example of role and responsibility.

Responsible	The department or person(s) responsible for developing and implementing the Procedure.	**The cyber security department**
Accountable	The person who has ultimate accountability and authority for the Procedure.	**Data owner**
Consulted	The person(s) or groups to be consulted prior to final Procedure implementation or amendment.	**Cyber security steering committee, Senior management**
Informed	The person(s) or groups to be informed after Procedure implementation or amendment.	**All employees, contractors**

v. **Procedure**

To facilitate co-ordination and consistency, organizations should have a core management committee that approves and authorizes all policies, procedures, protocols and guidelines formulated in the organization.

When the need for a procedure has been identified, and the mandate for the development of same has been received from either local or national management, the person or team responsible for the drafting of the procedure should initially identify the following:

- The background for the development of the procedure should be outlined.
- The overall purpose and objectives of the procedure must be described.
- The people and services to which the procedure applies must be identified.
- The extent of involvement of all stakeholders needs to be identified.

- The resources required to develop the procedure should be determined.
- The consultation process to meet our legal obligations to be followed.
- The communications process to support the early stages of procedure development needs to be outlined.

vi. **Related Document**

Here, identify any other documents that are relevant or important to the procedure. While all written material within the organization is related in one way or another, there will often be particular documents that should be read in conjunction with the procedures. To identify the related document organization can refer other policy, plan, procedure, guideline and protocols, you should also write a note what related document is used in the developing of the procedure.

vii. **Points of Contact**

Regarding procedures, the organization should assign a right person to give further information, clarity, and guidance for end-user. Assign the person that has detail and full information about the procedure and a person that has exact or related job description.

viii. **Definition**

Contains a list of themes used and uncommon words or words with meanings unique to the organization should be defined and listed in alphabetical order and list of unique terms, which by being defined would add clarity to the reader's understanding of the basic procedure.

- Define unfamiliar or technical terms
- Define terms with special meanings

To define those term organization can refer and adopt from cyber security national and international standards, policies, procedures, protocols and frameworks, like ISO27001 terms and definition.

ix. **Procedure Compliance**

a. Compliance Measurement

To measure the procedure compliance organization should select procedure compliance measurement mechanisms and methods including, but not limited to business tool reports, internal and external audits, and feedback.

b. Exceptions

Organization should define a responsible body for granting any exception to the procedure.

c. Non-compliance

An employee found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment.

x. **Revision History**

This section defines who is responsible for making updates and revisions to the procedure and how often these will take place. It may be useful to include a reference to the document as a living document which can be updated as determined by those responsible for updates and revisions. This will ensure that any ad hoc revisions are accounted for as well as scheduled updates. Information should also be included detailing where the procedure will be published and how employees can access it. The table below is example of the revision history information that contains.

Version	Description	From	to	Responsible/ Author	Summary of Revision
1.0	Initial version	Click or tap to enter a date.	Click or tap to enter a date.		

xi. **Reference**

The evidence base, listing the relevant references and the year published using Harvard style referencing and providing hyperlinks to associated procedures.

xii. **Appendices**

Forms, Records and other Associated Documentation will be attached to the procedure as Appendices and listed on the contents sheet at the front of the procedure. Appendices will be consecutively numbered, e.g. Appendix I, Appendix II.

9.5 Cyber Security Procedure Template

Cover letter:

Title: "Title of the Procedure"

Document reference number	
Revision number	
Approval date	
Revision date	
Document developed by	
Document approved by	
Responsibility for implementation	
Responsibility for revision and audit	

Document reference number:

Assign the reference number of the procedure.

Revision number:

Assign a number each time the document is revised.

Approval date:

Date when the procedure has been approved

Revision date:

Date the procedure is due for revision

Document developed by:

This should be the name of chair of the development group. The members of the working group should be listed as an appendix.

Document approved by:

This is the name of the Chair of the Core Management Committee who has final sign off.

Responsibility for Implementation:

Identify and name the individual who is responsible for rolling out the implementation of the procedure. This individual's job title should also be documented.

Responsibility for revision and audit:

Identify and name the person(s) with responsibility for revision and audit. This individual's job title should also be documented.

Introduction:

This section is an overview of the importance and role of the procedural documents. Provide background information that the procedure will address over the information technology (cyber) resources and capabilities that must be established and operated in order for those items to be considered secure.

Purpose:

In this section state the purpose of the document including the rationale for development of the procedure. This describes the objective for writing the procedure. It provides the rationale for why the procedure is required. Outline the objectives and intended outcomes of the process/system being described. It should be comprehensive and concise in its meaning.

Scope:

This identifies the users of the procedure. It identifies to whom the procedure applies. Specify area, function or personnel involved. This procedure… (Encompasses or applies to) (All, any, each):

Roles and Responsibilities:

Clearly define the appropriate personnel to fulfill the following roles and responsibilities in relation to the steps outlined in this procedure:

- Those responsible for complying with the procedure.
- Those responsible for ensuring compliance to the procedure.

Procedure:

Describes the overall objectives, functions, or tasks that the procedure is designed to accomplish and the circumstances under which the procedure should be used. Specific step by step directions from for example, a flow chart or task list outlined in a general sequence from start to finish.

Related Document:

Consider what are the other documents or references (policies, standards, procedures, forms, guidelines) are used to provide additional or further details about the "title of cyber security procedure".

Point of Contact:

This section is about assigning a responsible person who assists a user who has difficulties to understand or to implement "title of cyber security procedure".

Glossary of Terms and Definitions:

This section gives explanation of key technical terms or terminology that are referred to in the procedure.

- List definitions in alphabetical order. If this is an exhaustive.
- List then they may be included in an appendix.

Policy Compliance:

This part is a statement regarding the consequences of non-compliance with the procedure.

Revision and Audit:

The procedure should be reviewed and audited at an appropriate time after the procedure has been disseminated and implemented – this revision and audit date should be agreed by the committee developing the procedure at the time of final sign off.

- those responsible for revision the procedure
- those responsible for auditing the procedure and providing feedback to relevant employees

References:

List all references used in the procedure and include in the bibliography.

Appendices:

Additional information is included in this section that will support and provide a rationale for the procedure. This could include:

- Relevant diagrams
- Flow charts
- Models
- Each appendix should be incrementally numbered using roman numerical script (e.g. Appendix I, II, III, IV etc.)

10. Policy Guidelines

10.1 Overview

A guideline is an advisory document and a statement to determine a course of action. This aims to reorganize particular processes according to a set of routine or sound practice. The guideline elaborates more for the implementation of the policy and supports the easy use of procedure. Guideline is simply to give an overview of how to perform a task and should contain information that will be helpful in executing the procedure.

10.2 Considerations

Policies, procedures and guidelines are more successful when their implementation has been considered from the outset. Before developing a policy, procedure or guideline, consider the following:

- What do you want to achieve?
- What other strategies might help you achieve this?
- Is there a similar policy, procedure or guideline that covers this topic? How has this been implemented? Can it be amended to cover your issue?
- What is your target audience? How will you consult with them sufficiently to ensure that your document is practical and realistic?
- What resources might be needed for implementation?
- Are there any education and/or training requirements associated with implementation? If so, what will this entail and how will it be resourced?
- What are the risks of implementation versus leaving things as they are?
- What are the potential barriers to implementation?
- How will you let people know there's been a change in practice?
- How will you monitor effectiveness and compliance?

10.3 Methodology

Here are the components a guideline should have, but not limited to;

i. **Introduction**

Draw together the structure of the organization's policy guideline, and provides any other pertinent introductory statements required. It is a general overview about the cyber security policy guideline and what is all about addresses in this section.

ii. Objective

This section details the organization's policy guideline objectives, how these guideline objectives will be achieved and what resourcing will be supplied to support the implementation of the guideline. Refer to relevant information and look for words and phrases that tell the story about the subject or solution to the original problem statement.

Scope

The scope details any limitations or constraints on the applicability of the policy guideline to situations or entities within the agency. This policy guideline should be developed in conjunction (or consultation) with relevant business areas such as finance, audit and senior business management. Agencies should also ensure this policy guideline (and associated processes) adequately addresses security considerations relating to off-site work arrangements (e.g. home-based, mobile, regional, interstate and overseas).

iii. Guideline (Best practice)

List out and select a best practice which is highly applicable, advisable and recommended under the specific context and nature of the organization business.

iv. Roles and responsibilities

This section clearly specifies roles and responsibilities of individuals (listed in order of seniority) in relation to the development and implementation of the specific guideline. This will include the identification of a Chief Officer with overall responsibility for the particular guideline topic. To assign the role and responsibility organization can refer job description of departments, units, offices, individual employees. Also, refer Critical Mass Cyber security Requirement Standard this standard indicates what individual and managements need to do to secure their critical information and information system, specifically, in the Cyber Security Governance Process part of it.

v. Related Documents

This section identifies any other documents that are relevant or important to the guideline. While all written material within the organization is related in one way or another, there will often be

particular documents that should be read in conjunction with the guideline. Describe relevant legislation, standard, policy, procedure, forms or other document to the achievement of the objectives usually by providing additional details concerning specific topics.

vi. Definition

Define the meaning of key words or phrases used in the guideline which may not be familiar to, or might be misunderstood by a reader. To define those term organization can refer and adopt from cyber security national and international standards, policies, procedures, protocols and frameworks, like, ISACA Glossary, ISO27001 terms and definition.

vii. Reference

The evidence base, listing the relevant references and the year published using Harvard style referencing and providing hyperlinks to associated procedures.

viii. Appendices

Forms, Records and other Associated Documentation will be attached to the procedure as Appendices and listed on the contents sheet at the front of the procedure. Appendices will be consecutively numbered, e.g. Appendix I, Appendix II.

10.4 Cyber Security Policy Guideline Template

Cover page:

Title: "Title of the policy guideline"

Document reference number	
Revision number	
Approval date	
Revision date	
Document developed by	
Document approved by	
Responsibility for implementation	
Responsibility for revision and audit	

Document reference number:

Assign the reference number of the guideline.

Revision number:

Assign a number each time the document is revised.

Approval date:

Date when the procedure has been approved

Revision date:

Date the procedure is due for revision

Document developed by:

This should be the name of chair of the development group. The members of the working group should be listed as an appendix.

Document approved by:

This is the name of the Chair of the Core Management Committee who has final sign off.

Responsibility for Implementation:

Identify and name the individual who is responsible for rolling out the implementation of the procedure. This individual's job title should also be documented.

Responsibility for revision and audit:

Identify and name the person(s) with responsibility for revision and audit. This individual's job title should also be documented.

Introduction:

The introduction tells overview on the importance and role of the guideline documents. Provide background information that the procedure will address over the information technology (cyber) resources and capabilities that must be established and operated in order for those items to be considered secure.

Objective:

State the main goals of the policy; this will explain the reason for the policy guideline and will help readers understand how the policy guideline should be used. Legal and compliance issues should also be mentioned in here. Include statements on any specific legislation the policy guideline is designed to adhere to.

Scope:

The scope is a statement of the infrastructure and information systems to which the policy guideline applies, and the people who are stakeholders in it. Stakeholders would typically include anyone who is a user of the information or systems covered by the guidelines.

Best practice:

This section list out and identify the best practices which is widely applicable according to the organization context and business nature.

Roles and Responsibilities:

Clearly define the appropriate personnel to fulfill the guidelines. Identifies who is responsible for adhering to, implementing, and monitoring relevant aspects of the guidelines.

Related Documents:

In this section consider what are the other documents or references (policies, procedures, forms, guidelines, standards) were used to provide additional or further details about the "title of cyber security guideline".

Definition and Acronym:

Define meaning of key or unique terms used in the guideline which may not be familiar to, or might be misunderstood by a reader.

References:

List all references used in the procedure and include in the bibliography.

Appendices:

Additional information is included in this section that will support and provide a rationale for the procedure. This could include:

- Relevant diagrams
- Flow charts
- Models
- Each appendix should be incrementally numbered using roman numerical script (e.g. Appendix I, II, III, IV etc.)

11. Strategic plan

11.1 Overview

In development and implementation of cyber security strategic plans, there are vital subjects that discuss about how to develop and implement it efficiently and effectively. For instance, here are some of the subjects; phases of strategic plan and main activities, workflow, resources and responsible bodies.

The action plan should lay out the activities and budget of the strategy as well as the responsible bodies for each part. For instance, the action plan clarifies the responsible body to whom the report of the action plan should be submitted and also justifies the feasible strategy duration, cost of the strategy, and the activities of the action plan that should be reflected in the work plans of the various sectors and/or units. The workflow of the plan should clearly articulate who do what and how. Also, redefines strategy outlines and objectives with their cyber security perspectives, which have been stated in strategy section implementing a cyber-security strategic plan typically requires one or more projects or initiatives. Correspondingly, organization should has portfolio management that help to determine when and how to develop and implement a collection of cyber security programs, projects and/or other initiatives, which facilitate main activities, to achieve strategic objectives. In addition, organization should state how it is going to accomplish the goal and explain performance indicators.

Furthermore, gap analysis, an analysis of the gap between the current state and the desired state for each defined metrics, help identify the requirements and priorities needed for an overall plan or road map to achieve the objectives and fill the gaps.

11.2 Steps to Develop Strategic Plan

As stated on Critical Mass Cyber Security Requirement Standard version 1.0(2009E.C), organizations should follow cyber security planning process and its core principles to develop a cyber-security strategic plan that best suits them. The following steps help while developing cyber security strategic plan:

Step 1: Initiating the Plan

The organization should identify specific issues the strategic plan should address. Issues like, clearly defined roles and responsibilities, organizational profile, the information that should be collected to help make sound decisions.

Step 2: Developing a Mission and Vision

Mission Statement: A mission statement reflects the essence of an organization's cyber security intent and tells when, where and how it should fulfill its purpose.

Vision Statement: A descriptive sentence that presents a broad image of what success should look like for the organization's cyber security issues.

Step 3: Conducting an Environmental Assessment

The reason for conducting environmental assessment is to help understand the overall and current situation of the organization with respect to cyber security issues. This step is about gathering up to date information about the organization. As a result, the cyber security strategic plan will reflect the organization's strength it possesses (possessed cyber security capabilities to be further exploited), gaps it needs to fill (cyber security capabilities help doing so), opportunities it can exploit to reach its desired state and challenges it has faced. Meaning, the cyber security strategic plan can easily highlight the critical cyber issues the organization faces and gives direction on how to address such issues.

Step 4: Evoking or Developing Strategy, Goals and Objectives

The general and specific results to be sought the goals and objectives. Goals and objectives should come from individual inspiration, group discussion or formal decision making techniques. This can take considerable time. Discussions at this stage frequently require additional information or a reevaluation of conclusions reached during the environmental assessment. It is even possible that new insights emerge that change the thrust of the mission statement. To create the best possible plan it is important that the delegated body not be afraid of going back to an earlier step in the process to take advantage of newly available information.

Step 5: Writing the Strategic Plan

After the organization articulated its mission, identified the critical issues, and agreed upon the objective. So this step essentially involves putting all that down on paper. To write strategic plan,

organization should refer to strategic plan template, acceptable organizational or national or international writing format standard in combination.

11.3 Methodology

Here are some of the requirements should be considered while developing a strategic plan, but not limited to;

i. **Introduction**

This part is a brief explanation of the subjects of the strategic plan and the context of the publication. To describe the overview of the strategic plan, organization should refer their mission and vision, other internal documents, national and international procedures, like Critical Mass Cyber security Requirement Standard.

ii. **Goal**

Describe the strategic goals which are planned objectives that an organization strives to achieve. Such strategic goals should be achievable and should reflect a realistic assessment of the current state and projected desired state.

In order to set strategic goals, organization must be sure that the goals are focused on the important aspects of implementing the strategy. Be careful not to set too many goals that run the risk of losing focus. Also, design their goals so that they do not contradict and interfere with each other.

The goal should be understandable (simply and easy to understand), suitable (assist in implementing the strategy), acceptable (fit with the values of the organization), flexible (it be adaptable).

iii. **Objective**

An objective is a precise, measurable, time phased result that supports the achievement of a goal. The product of this step is a justification of the organization's strategic outline and directions. The objectives should be defined and metrics developed to determine if those objectives are being achieved.

iv. **Directions**

The organization should state strategic directions in outline format. This section contains the strategy statement which is found on the organizational cyber security strategy document.

v. Roles and Responsibilities

To assign the role and responsibility organization should refer duties of management board, Management Committee and the necessary staffs' job description given by proclamation and/or regulation. Also, refer Critical Mass Cyber security Requirement Standard which indicates responsible body and organizational entity.

vi. Gap Analysis

The analysis should identify the steps needed to move from the current state to the desired state to achieve the defined objectives. Doing so may need to be repeated frequently as much as needed to provide performance and goal metrics, and information on possible midcourse corrections needed in response to changing environments or other factors. A typical approach to gap analysis is to work backward from the endpoint to the current state and determine the intermediate steps need to accomplish the objectives.

Organization should employ optimum methods that can be used to assess the gap between the current and desired state. Some typical areas that should be assessed and /or ensured include:

- A security strategy with senior management acceptance and support.
- A security strategy intrinsically linked with organizational business objectives.
- Security policies those are complete and consistent with strategy.
- Complete standards for all relevant, consistently maintained policies.
- Complete and accurate procedures for all important operations.
- Clear assignment of roles and responsibilities.
- An organizational structure ensuring appropriate authority for cyber security governance and management without inherent conflicts of interest.
- Information assets that have been identified and classified as criticality and sensitivity.
- Effective controls that have been designed, implemented and maintained.
- Effective security metrics and monitoring processes, in place.
- Effective compliance and enforcement processes.
- Risk that is properly identified, evaluated, communicated and managed.
- Adequate security awareness and training of all stakeholders.
- The development and delivery of activities that can positively influence security orientation of culture and behavior of staff.

- Regulatory and legal issues third-party service providers.
- The timely resolution of noncompliance issues and other variances.
- Tested business continuity and disaster recovery plan.
- Appropriate security approvals in change management processes.

vii. **Action Plan**

The prepared cyber security strategic plan mentioned and discussed in the above section should be put into ground. Consequently, this strategic plan should consist action plan that state specific actions or activities that used to achieve a goal within the constraints of the objective. To do so, action plan that includes gap analysis, cyber security program development, performance measures and other related subjects should be included.

Organization should engage gap analysis that is a basis for an action plan programs based on organizational policy, international and national standards. And, the action plan should consider the necessary training, awareness programs and action plan metrics such as key goal indicators, key performance indicators, critical success factors, and general metrics. For further illustration, here in the following there are vital subjects (but not necessarily limited to them) should be incorporated in the process of implementing cyber security strategic plan:

viii. **Develop Programs**

The most important aspect of the action plan is to execute the strategic plan. The programs listed on the action plan to help execute the strategic plan should follow standards that help guide and determine content, format and requirements of the programs. Also consider policies associated with the programs.

a. Develop Policies

As a strategy evolves, it is vital that supporting policies are developed to articulate the strategy. For example, if the objective is to become CMCSRS compliant over a five year period, then the strategy must consider which elements are addressed first, what resources are allocated, how the elements of the standard can be accomplished and so forth. The road map should show the steps and the sequences, dependencies and milestones. The action plan is essentially a project plan to implement the strategy following the road map.

If the objective is CMCSRS compliance, each of the relevant five (5) capabilities building and thirty-two (32) main processes focus areas should be the subjects of a policy. In practice, this can

be effectively accomplished with about many specific policies for even large organizations. Each of the policies is likely to have a number of supporting standards typically divided by security area. In other words, a set of standards for a high-security area should be more stringent than the standards for a low-security area. Other standards should need to be developed for different business units, depending on their activities and regulatory requirements.

The complete strategy provides the basis for creation or modification of existing policies. The policies should be directly traceable to strategy elements. If they are not, either the strategy is incomplete or the policy is incorrect. It should be apparent that a policy that contradicts the strategy is counterproductive. The strategy is the statement of intent, expectations and direction of governance and management. The policies should, in turn, be consistent with and support the intent and direction of the strategy.

b. Develop Standards

Organization should develop standards that serve to interpret policies of strategy intent so that they reflect the intent of policy. These standards should be disseminated to those governed by them as well as those impacted. Review and modification processes should be developed as well. A process for implementing compensatory controls should be developed for out of compliance situations.

i. **Prepare Training and Awareness**

An effective action plan to implement a security strategy should consider an ongoing program of security awareness and training. To ensure awareness of new or modified policies all impacted personnel should be trained appropriately in order for them to see the connection between the policies and standards and their daily tasks or activities.

In addition to providing information to those impacted by changes, it is important to ensure that employees involved in the various aspects of implementing the strategy are also appropriately trained. This includes understanding the objectives of the strategy, the processes that should be used and performance metrics for the various activities.

ii. **Determine Performance Metrics**

The plan of action to implement the strategy requires methods to monitor and measure progress, and the achievement of milestones. As with any project plan, progress and costs should be monitored on an ongoing basis to determine conformance with the plan and to allow for midcourse

corrections on a timely basis. There are likely to be a variety of near term goals each requiring resources and a plan of action for achievement.

Considerations for cyber security metrics include ensuring that what is being measured is, in fact, relevant. Because security is difficult to measure in any objective sense, relatively meaningless metrics are often used simply because they are readily available. Metrics serve only one purpose, providing the information necessary for making decisions. It is therefore critical to understand what decision should be made, who makes them and then find ways of supplying that information in an accurate and timely fashion. Different metrics are more or less useful for different parts of the organization, and should be determined in collaboration with business process owners and management.

There are a number of approaches that can be used for ongoing monitoring and, measurement of progress. One or more of the methods used to determine current state can be used on a regular basis to determine and chart how progress of current state has changed. For illustration, the plan of action to achieve regulatory compliance for CMCSRS implementation manual should require, the organization's cyber security strategy plan implementation possible monitoring and metrics include the following among other things such as a detailed analysis by competent personnel to determine regulatory requirements for affected business units; knowledge of current state of compliance and definition of required state of compliance. In addition, each plan of action benefit from developing an appropriate set of key performance indicators, defining critical success factors and setting agreed upon key goal indicators.

Being mindful of the notion that, metrics design and monitoring activities should take into consideration what is important to manage information security operations and what senior management wants to know. Organization should determine strategic metrics interested information of a strategic nature by forecasting further tactical and operational metrics. A senior management typically wants a summary of information important from a strategic perspective that includes progress according to plan and budget; significant changes in risk and possible impacts to business objectives. Improvements in overall monitoring can be achieved by careful analysis of available metrics to determine their relevancy.

iii. **Definition**

Contains a list of themes used and uncommon words or words with meanings unique to the organization should be defined and listed in alphabetical order and also, list unique terms that, by

being defined, would add to the reader's understanding of the basic strategic plan. Define unfamiliar terms, technical terms and terms with special meanings.

To define those term organization can refer and adopt from cyber security national and international frameworks, like organizational regulation, definition on proclamation document.

iv. **Relevant Documents**

Organization should list all documents cited in strategic plan and relevant to provide additional or further details about the plan.

v. **Appendices**

This section may include explanation of key technical terms or terminology that are referred to in the strategic plan and lists of references used in the plan development. This may described by diagrams, flow charts or models. Each appendix recommends to be incrementally numbered using roman numerical script (e.g. Appendix I, II, III, and IV etc.).

11.4 Cyber Security Strategic Plan Template

Cover Letter:

Title: "Title of the Strategic Plan"

Document reference number	
Revision number	
Approval date	
Revision date	
Document developed by	
Document approved by	
Responsibility for implementation	
Responsibility for revision and audit	

Document reference number:

Assign the reference number of the strategic plan.

Revision number:

Assign a number each time the document is revised.

Approval date:

Date when the strategic plan has been approved

Revision date:

Date the strategic plan is due for revision

Document developed by:

This should be the name of chair of the development group. The members of the working group should be listed as an appendix.

Document approved by:

This is the name of the Chair of the Board or Core Management Committee who has final sign off.

Responsibility for Implementation:

Identify and name the individual who is responsible for rolling out the implementation of the plan. This individual's job title should also be documented.

Responsibility for revision and audit:

Identify and name the individual/organizational entity with responsibility for revision and audit. This individual's job title should also be documented.

Tip: In general, the cover letter from the president/chair of the board of directors introduces the strategic plan. It gives the strategy a stamp of approval and demonstrates that the organization has achieved a critical level of internal agreement.

Introduction:

Organization should state about the cyber security strategic plan. Organization should describes about the general over view of the organizational cyber security strategic plan document. The overview of strategic plan should be completed last, and under this section organization should merely summarizes each of the other sections of the plan.

SWOT Analysis with PESTEL

Organization should analyze the strength, weaknesses and identify opportunities and threats (SWOT) with political, economic, social, technological, legal and environment (PESTEL) of the organization. Consequently, it clearly states the current status of organization. Organization should consider and determine strategy planning process enablers that assist to develop a cyber-security strategic plan. (Refer cyber security strategy document).

Determine Objective and Key Strategic Goal

Organization should use strengths, weaknesses, opportunities, and threats (SWOT) analysis with political, economic, social, technological, legal and environment (PESTEL) in order to determine objectives or desired state. Map the routes and steps that should be taken to navigate to the objectives of the strategy. (Refer cyber security strategy document).

State Mission and Vision

Organization should clearly put statements of mission, vision, values and another related issues.

- **Mission**: should explain what the organization seeks to accomplish and why it exists and the desired result of its efforts in cyber concern.
- **Vision**: Vision statements provide clarification for the future of the organization, and should be inspirational.

Action Plan to Implement Strategy

Organization should determine methodology that enables to clarify strategy's vision and translate it into action. Organization should prepare action plan in order to implement cyber security strategy. Organization should determine methodology of aspects action plan. Here are important aspects such as:-

- **Gap Analysis**: analyze the gap between current state and desired state.
- **Policy and Standard Development**: organization should create or modify policies and standards as needed.
- **Training and Awareness**: organization should consider an ongoing program of security awareness and training.
- **Action Plan Metrics**: organization should conduct methods to monitor and measure progress and achievement of milestones.

Roles and Responsibilities:

Clearly define the appropriate personnel/organizational entity to fulfill the strategy plan. Identifies who is responsible for adhering to, implementing, and monitoring relevant aspects of the strategic plan.

Relevant Documents:

Organization should list all documents cited in strategic plan and relevant to provide additional or further details about the plan. In this section consider what are the other documents such strategy and CMCSRS use to provide additional or further details about the "title of cyber security strategy plan".

Appendices:

Additional information is included in this section that will support and provide a rationale for the procedure. This section also includes definition of key or unique terms used in the guideline which may not be familiar and list of references used in the strategic plan. This section may derived by: diagrams, flow charts and models. Each appendix should be incrementally numbered using roman numerical script (e.g. Appendix I, II, III, IV etc.)

12. Strategy

12.1 Overview

The cyber security strategy should include main tasks and knowledge needed to do tasks. A strategy for achieving defined outcomes for the cyber security program is necessary to develop an effective, mature security program. It should support a leadership and guide a development of strategic requirements, policies and standards. Ultimately, the strategy should provide a basis for a road map for its implementation and put performance metrics.

Similarly, the process of developing an effective cyber security strategy requires a thorough understanding and consideration of a number of elements. In addition, it is also important for the cyber security manager to be aware of the common failures of strategic plans.

Besides, the strategy provides the basis for an action plan comprised of one or more security programs that, as implemented, achieve the security objectives. The action plan must be formulated based on available resources and constraints, including consideration of relevant legal and regulatory requirements.

To be effective, the strategy should consider a variety of factors, including the available resources as well as the constraints. Also, the strategy should forecast the upcoming cyber-security strategic plan.

Organization should adopt a cyber-security strategy articulate coordinated approach or direction in order to achieve the defined objectives that result in the desired outcomes, utilizing available resources within changing the existing constraints into opportunities.

12.2 Methodology

Here are the components a strategy should have, but not limited to;

i. Introduction

Describe the general introduction of the organizational cyber security strategy document. To write the introduction of this strategy organization can refer Critical Mass Cyber Security Requirement Standard, organizational strategy, organizational main powers and duties and other related documents regard to Cyber security.

ii. Purpose

This section describes about the purpose of the strategy document.

iii. Determine Strategy Elements

A set of cyber security objectives coupled with available processes, methods, tools and techniques create the means to construct a security strategy. Express how to identify and state resources or constraints. Furthermore, identify how to change constraints into resources.

Organization should know where one is and where one is going. Which essentially provides the starting point for strategy development; it provides the framework for creating a road map. A road map is the steps that should be taken to implement the strategy.

The typical roadmap to achieve a defined, secure desired state includes people, processes, technologies and other resources and enablers. The over all interaction and relationship between the various elements serves to map the routes and steps that should be taken to navigate to the objectives of the strategy. Enablers can function as resources as well as constraints and should be considered from both perspectives.

iv. Resources

To the extent possible, the strategy should use existing resources in order to maximize utilization of existing assets and capabilities. Typically, they include but not limit to:

- **Frameworks** are the vehicle to translate the desired behavior into practical guidance for leadership.
- **Processes** describe an organized set of practices and activities to achieve certain objectives.
- **Organizational structure** is the key decision making entities.
- **Culture, ethics and behavior** are success factor in governance and management activities
- **People, skills and competencies** are linked to people and are required for successful completion of activities and making correct decisions and taking corrective actions.

v. Constraints

There are also a number of constraints that should be considered when developing a security strategy and subsequent action plan. Typically, they include but not limit to:

- **Legal:** laws and regulatory requirements
- **Physical:** capacity, space, environmental constraints
- **Ethics:** appropriate, reasonable and customary

- **Culture:** both inside and outside the organization
- **Costs:** time, budget
- **Personnel:** resistance to change, resentment against new constraints
- **Organizational Structure:** how decisions are made and by whom
- **Resources:** capital, technology, human power
- **Capabilities:** knowledge, training, skills, expertise

vi. Analysis of Current State

This section of the intended strategy describes systematic collection and evaluation of past and present organizational cyber security status aimed at:-

- Identification of internal and external forces that may influence the organization's cyber security performance and choice of strategies, and
- Assessment of the organization's current cyber security strengths, weaknesses, opportunities, and threats.

vii. Desired State

This part contains the state that the organization want to arrive by considering different cyber security issues mean complete snapshot of all relevant conditions at a particular point in the future. To clearly define the desired state, the organization should place the current capability maturity level based on the critical mass cyber security requirement standard road map.

viii. Recall Organizational Strategy and Previous Cyber Security Strategy

Refer organizational strategy; express why and how to recall them and make link with cyber security strategy. Refer pervious cyber security strategy and determine how to link with new one.

ix. Define Main Outlines of Cyber Security Strategy

The outline of a cyber-security strategy should fully implement relevant components of CMCSRS. Put best approaches that are appropriate for defining the desire state of security. Employ a combination of methods to outline strategy to assist in communications with others and as a way to crosscheck the objectives to make certain all relevant elements are considered. Describe desired states and outline cyber security strategies well.

As well, to ensure that all relevant elements of security addressed in an organizational security strategy, major headings of CMCSRS must be considered, but does not necessarily limited to them.

For example, leadership capability building, human capability building and the 3 (three) strategic management processes (disruptive change management process, disruptive risk management process, cyber security strategy and policy development process) can provide a useful framework to gauge comprehensiveness. In similar fashion, the main cyber security perspectives targets of CMCSRS such are human, process, structure and technology should be taken into account to satisfy the state objectives and goals of cyber security.

In another hand, it is also important to be aware of the common failures of strategic plans. Experiments and studies have shown a variety of underlying causes for flawed decision making that causes of strategy failures. Being aware of them may allow compensation to reduce adverse effects. Some of the main reasons include:

- **Overconfidence:** Research shows a tendency for people to have excessive confidence in the ability to make accurate estimates. But, for organizational strategies based on assessments of core capabilities, this can be particularly troublesome.
- **Optimism:** Research shows that once a number of people tend to be optimistic in their forecasts. A combination of overconfidence and over optimism can have a disastrous impact on strategies based on estimates of what may happen.
- **False Consensus:** there is a well-documented tendency for people to overestimate the extent that others share their views, beliefs and experiences. When developing strategies, false consensus can lead to ignoring or minimizing important threats or weakness in the plans and to persisting with doomed strategies.

x. Make Symbiotic as Parts of Organizational Strategy

Establish and maintain a cyber-security strategy in alignment with organizational goals and objectives to guide the establishment and ongoing management of the cyber security program. Integrate cyber security leadership into corporate level to ensure that organizational goals and objectives are supported by the cyber security programs. In order to do so organization should:

- Define security strategy linkages to organizational functions.
- Express the relationship between cyber security and the objectives of the organization.
- Relate information security program objectives to organizational objectives.
- Define the outcomes of cyber security that support organizational objectives.

xi. Put Direction How to Interpret into Activities

Illustrate how to interpret the strategy into programs such as policy, strategy plan, tactic plan and operation plan. As well, while developing cyber security strategy, organization should foretell the further future of strategy and consider into account how to interpret into activities.

xii. Roles and Responsibilities

Clearly specify the roles and responsibilities of individuals (listed in order of seniority) in relation to the development and implementation of the specific guideline. This will include the identification of a Chief Officer with overall responsibility for the particular guideline topic and may also include reference to the role of the Board or a Committee. To assign the role and responsibility organization can refer job description of departments, units, offices individual employees. Also, refer to Critical Mass Cyber security Requirement Standard this standard indicates what individuals and management need do to secure their critical information and information system.

xiii. Related Documents

This section identifies any other documents that are relevant or important to the strategy. While all written material within the organization is related in one way or another, there will often be particular documents that should be read in combination with the strategy.

xiv. Definition and Acronym

Define the meaning of key words or phrases used in the strategy which may not be familiar to, or might be misunderstood by a reader. To define those term organization can refer and adopt from cyber security national and international standards, and frameworks, like Information Security Governance, organizational proclamation and regulation.

xv. Appendices

This section may include explanation of key technical terms or terminology that are referred to in the strategy and lists of references used in the strategy development. This may described by diagrams, flow charts or models. Each appendix recommends to be incrementally numbered using roman numerical script (e.g. Appendix I, II, III, and IV etc.).

12.3 Cyber Security Strategy Template

Cover Letter:

Title: "Title of the strategy"

Document reference number	
Revision number	
Approval date	
Revision date	
Document developed by	
Document approved by	
Responsibility for implementation	
Responsibility for revision and audit	

Document reference number:

Assign the reference number of the strategy.

Revision number:

Assign a number each time the document is revised.

Approval date:

Date when the strategy has been approved

Revision date:

Date the strategy is due for revision

Document developed by:

This should be the name of chair of the development group. The members of the working group should be listed as an appendix.

Document approved by:

This is the name of the Chair of the Board or Core Management Committee who has final sign off.

Responsibility for Implementation:

Identify and name the individual who is responsible for rolling out the implementation of the strategy. This individual's job title should also be documented.

Responsibility for revision and audit:

Identify and name the individual/organizational entity with responsibility for revision and audit. This individual's job title should also be documented.

Tip: Besides, a cover letter from the president of the board of directors introduces the strategy. It gives the strategy a stamp of approval and demonstrates that the organization has achieved a critical level of internal agreement.

Introduction:

In one to two pages, this section summarizes the strategy. It should reference the strategy enablers, organization profile and strategy's perspectives.

Strategy Resources and Constraints:

Articulate the cyber security strategy enablers such as resources and constraints. It should be comprehensive and concise in its meaning.

Organization's Profile:

In one or two pages state the history of organization in issues of cyber security such as key events, achievements and changes over time.

Outlines of Strategy

This section makes explicit the strategic perspectives and the critical issues behind the strategy. The section should be presented as a brief outlines of strategy that covers several pages. Describe the alignment of the strategy's outlines with organizational objective.

Roles and Responsibilities:

Clearly define the appropriate personnel to fulfill the following roles and responsibilities in relation to the steps outlined in this strategy.

Relevant Documents:

This section provides all relevant and referenced documents in the process of cyber security strategy development. Consider what are the other documents, regulations, proclamation uses to provide additional or further details about the "title of cyber security strategy".

Appendices:

Additional information is included in this section that will support and provide a rationale for the strategy. Besides, this section may include explanation of key technical terms or terminology that are referred to in the strategy and lists of references used in the strategy development. This may

described by diagrams, flow charts or models. Each appendix recommend to be incrementally numbered using roman numerical script (e.g. Appendix I, II, III, IV etc.).

13. Cyber Security Tactical Plan

13.1 Overview

Cyber Security Tactical Plan takes an organization's Cyber Security Strategic Plan and sets forth specific short-term actions and plans. It supports strategic plans by translating them into specific plans relevant to distinct business areas of the organization. Cyber security business unit managers use the cyber security tactical planning to outline what the various parts of the organization must do regarding the issues of cyber security for the organization to be successful at some point into the future, for example, in one year. The tactical planning horizon is shorter than the strategic plan horizon. If the strategic plan is for five years, tactical plans might be for a period of one to three years, or even less, depending on what kind of market the business serves and the pace of change. So the Cyber Security Tactical Plan emphasizes analyzing the everyday functions of the organization cyber security issue. Flexibility needs to be built into tactical plans to allow for unexpected events to be measured and preparation regarding handling consequential changes following the unexpected events be addressed to reach the goals and objectives of the strategic plan.

The tactical plan should be prepared based on CMCSRS Cyber Security Planning Process, Requirement D1.

13.2 Consideration Areas and Steps

Questions need to be addressed when developing tactical plans include:

- How can the strategic goals be achieved within the existing resources?
- What daily, weekly, monthly and yearly actions accomplish the preferred outcomes?
- What part does each person/department play in making these tactics work?

1. Review the organization overall CS strategic plan then sets forth specific short-term actions and plans
2. Identify the what the various parts of the organization can responsible for each tactical plan - divide the existing strategy and assign it to each department or unit of organization
3. Allocate resource for each tactical plan
4. Decide what each department should accomplish in terms of a tactic or action item
5. Assign an allotted time to each tactical plan.

Effective tactical planning depends on many factors, which vary from one situation to another. First, the manager needs to recognize that tactical planning must address a number of tactical goals derived from strategic goals. An occasional situation may call for a stand-alone tactical plan, but most of the time tactical plans flow from and must be consistent with a strategic plan. Second, although strategies are often stated in general terms, tactics must specify resources and time frames. A tactical plan must specify precisely what activities will be undertaken to achieve the goal. Finally, tactical planning requires the use of human resources. Managers involved in tactical planning spend a great deal of time working with other people. They must be in a position to receive information from others within and outside the organization, process that information in the most effective way and pass it onto others who might make use of it.

13.3 Methodology

i. Introduction

Briefly explain the subjects of the tactical plan and overview point Cyber Security Strategic Plan, which emphasizes on strategy goals. The tactical plan issues can be found in the Action Plan section of the Cyber Security Strategic Plan. Where, on this section, organizational responsible bodies and targeted specific set of strategy plan are expected to be clearly stated. The 'Introduction' section describes about the general over view of the organizational Cyber Security Tactical Plan and all the issues it addresses. Provide background information of the result of a prior tactical plan and which specific plan will the tactical plan addresses from strategic plan.

ii. Strategic Goals

This section describes about strategic goals, which are the planned objectives that an organization strives to achieve. Such goals drive from strategic plan then set its forth specific short-term actions and plans, specific strategic plans goals should be achievable and should reflect a realistic assessment of the current and projected business environment. Include outcome, date to be completed.

iii. Strategy Governances

Identifies who within organization are Responsible, Accountable, Informed or Consulted with regards to this tactical plan. The following definitions apply:

iv. Action Plans

Describe about action plan which is statements of specific actions or activities that will be used to achieve a goal within the constraints of the objective. Manage and assign appropriate resource that are need to performing action plan regarding its human resource, budget, time and other that are influencing direct or indirect the strategy goals.

v. Implementation Time Table

Contain break down strategic goals periodically the annual, monthly. Outline what the various parts of the organization doing well define strategy plans goals with defined timeframe. It predicate or emphasizes the everyday functioning of the organization to cyber security operational plans.

13.4 Cyber Security Tactical Plan Template

Cover letter:

Title: "title of cyber security tactical plan".

Document reference number	
Revision number	
Approval date	
Revision date	
Document developed by	
Document approved by	
Responsibility for implementation	
Responsibility for revision and audit	

Document reference number:

Assign the reference number of the tactical plan.

Revision number:

Assign a number each time the document is revised.

Approval date:

Date when the tactical plan has been approved

Revision date:

Date the tactical plan is due for revision

Document developed by:

This should be the name of chair of the development group. The members of the working group should be listed as an appendix.

Document approved by:

This is the name of the Chair of the Core Management Committee who has final sign off.

Responsibility for Implementation:

Identify and name the individual who is responsible for rolling out the implementation of the policy. This individual's job title should also be documented.

Responsibility for revision and audit:

Identify and name the person(s) with responsibility for revision and audit. This individual's job title should also be documented.

Overview:

This section should describe, define and explain in clear terms about the "title of cyber security tactical plan". It is a general overview about the "title of cyber security tactical plan" and what is all about addresses in this section. Provide background information that the plan will address over the information technology (cyber) resources and capabilities that must be established and operated in order for those items to be considered secure.

Strategic Goals:

Describe about the strategic goals which is the planned objectives that your organization strives to achieve. What the organization is plan to achieve the strategy. List out what results that the organization wants to change in order to better meet their mission and to help resolve strategic issues. It should describe the responsibility and functionality of lower-level departments to achieve their strategic plan.

Action Plan:

In this section it should describe about action plan which is statements of specific actions or activities that will be used to achieve a goal within the constraints of the objective. It should describe what specific action will used to address the cyber security issue of the organization and should outline the detailed action needed to achieve the tactical plan.

The following are some of action to be describes

- A set of objectives that support the cyber security tactical plan

- A set of measurable goals that support the objectives
- A time-based schedule for achievement of goals
- A visible method of communicating what is to be done
- Accountable people for delivering each objective
- Clear milestones for objectives

Implementation Time Table:

In this section it should describes annual activities break down in monthly, what tasks are done, at what time, who will take responsibility for the task, what are the potential barriers individual or the organization might resist and what methods will use.

14. Cyber Security Operational Plan

14.1 Overview

Operational Plan does present highly detailed information specifically to direct people to perform the day-to-day tasks required in the running the organization. Organization management and staff should frequently refer to the operational plan in carrying out their everyday work. The Operational Plan provides the what, who, when and how much:

- **what** - the strategies and tasks that must be undertaken
- **who** - the persons who have responsibility of each of the strategies/tasks
- **when** - the timelines in which strategies/tasks must be completed
- **how much** - the amount of financial resources provided to complete each strategy/task

Operational Plan:

- A specific plan for the use of the organization's resources in pursuit of the strategic plan.
- Details specific activities and events to be undertaken to implement strategies
- Is a plan for the day-to-day management of the organization
- An operational plan should not be formulated without reference to a strategic plan
- Operational plans may differ from year to year significantly
- The operational plan is produced by the chief executive and staff of the organization.

The purpose of the Operational Plan is to provide organization how a personnel, team, section or department with a clear picture of their tasks and responsibilities to the achievement of the organization's Cyber security strategic goals stated on Strategic Plan. It is a management tool that facilitates the co-ordination of the organization's resources (human, financial and physical) so that goals and objectives in the strategic plan can be achieved.

14.2 Process Map of Operational Plan

This plan should be prepared based on CMCSRS Cyber security planning process requirement E1 - E3.

Step 1: Determine Goals and Objectives

Step 2: Determine what needs to be done to achieve each objective. (See note 1)

Step 3: Assign responsibility for each strategy and each task to one or more persons within the Organization. (See Note 2)

Step 4: Work out costs and physical resource need in involving undertaking each strategy and completing each task

Step 5: Determine timelines for completing all strategies

Notes:

1) Each objective may require more than one strategy and many tasks to be successfully completed.
2) Unless people are assigned responsibility, strategies and tasks are unlikely to be done.
3) Step 1 &2 from strategy planning.
4) From step 3 to 6 operational planning.

14.3 Methodology

i. Content

The Cyber security operational Plan usually contain the following information [But not limited to]:

ii. Introduction

In this gives a brief explanation of the subjects of the operational plan and overview point cyber security tactical plan, emphasizing the current operations of various parts of the organization and operational assessments, and its intended goals. This section also describe the establishment operation plan (it can be work plan) and what strategy goals achieve on this operation period. Describe about what are organizational cyber security operational plan, provide status of operational plan and what it addresses in this section. Describe what are, who are, which strategy operational plan.

iii. Scope

Determine the scope of operational plan, it may be developed from two directions one from boundary of applicability in order to define what, where, when, how, who and how much the operational plan should be applied. The other is from the view of which system and what type of activities should be done on the systems.

iv. Operational Goals

This section describes about operational goals which is the planned objectives that an organization strives to achieve. Goal of operational plan to achieve a strategies and tasks that are undertaken this operational plan period (section), set a strategies/tasks timelines, such strategic goals should be achievable and should reflect a realistic assessment of the current and projected business environment.

v. Specific Goals

Describe the address of operation action that identify specific goals that are achieves in short period and plan targeted outcome, that are help or support main goal of operational plan, the actions undertaken to implement strategies and it intended, goals that motivate responsible one tangible. Goal is defined as one that is specific, measurable, achievable, results-focused, and time- bound.

vi. Drivers of the operational plan

This section describes major push factors which drives organization to develop operational plan. Scanning or identify who, what are internal and external influence that impose or initiate organization to develop operational plan.

vii. Current State analysis

The organization analyze current state cyber security tactical plan emphasizes specific short-term actions and plan, and operation plan using operation related clauses ISO 27001(operation, support and other relevant clauses), it consider competence human power, budget, assets, and time.

viii. Measures required to achieve goals

Describe the required action to achieve goal that are mentioned on tactical plans, it is specific short-term actions and plans to achieve a specific goal.

ix. Human resources

Describe required professional, experience and number of man power need to allocating properly in each operational action, based on complexity of strategy of goals and career path.

x. Physical resources

Describe required physical resource in each operational actions, defined available and identify required resource or equipment that assets, it support operational plan role and responsible body and maintaining strategy goals.

xi. Budget/finance/

Allocating budget for a specific action, many strategies goals will involve administration costs, some will need purchases of equipment, or materials, or promotional costs such as advertising.

xii. Performance Indicators

Describe Performance Indicators of operational plan action, it is standard or reference point that allows management to measure the actual result of strategies and make comparisons between desired results and actual results.

xiii. Implementation timetables

Contain the break down activities that are describe implementation/operation/ period of strategy goals. Determine the actions or operation of each goals with respect of when, who, will take responsibility and well planned done.

14.4 Cyber Security Operational Plan Template

The Cyber security operational plan usually contains the following information [But not limited to]:

Introduction

This section should describe, define and explain in clear terms about the cyber security operational plan, provide status of operational plan and what it addresses in the entire plan. This section also, describes organizational cyber security tactical plan about that are initial points operation plan and operational risk assessments.

Scope

Covers security issues of the organization operational levels who, when, and how much resource needs to achieve the goals.

Operational Goals

Describes about Operational goals which are specifies specific to the daily tasks and requirements to run a business, to achieve organization planned objectives. It can be specific, measurable,

achievable, realistic, and time constrained. Operational Plan is clearly demonstration the implementation of strategies contained within the Strategic Plan.

Specific Goals

This section describes specific goals the organization that realize map achieve overall all strategic achievement of organization, goals must be clear and well defined, it provide sufficient direction operational procedure, and lowest levels of the organization contribute to achieve of strategic plan. Make it as easy as you can to get where you want to go by defining precisely where you want to end up. A specifically states well follows procedure, actions, starting and completed date of strategic planned objective/goal/, and expected degree of achievement of goal.

Drivers of the Operational Plan

In this section, factors, which drive to the development the cyber security operational plan are clearly described as per stated in tactical plan and organizational operational risk assessment. Tactical plan emphasizes the current operations of various parts of the organization, situations about current operational performance of the responsible body and impacts of operational performance and success of the goal.

Current State Analysis

In this section the organization analyze cyber security operation plan using operation related clauses ISO 27001(operation, support and other relevant clauses), it consider competence human power, budget, assets, and time.

Measures Required to Achieve Goals

- Identify information like; man power, resource (asset) is needed to meet that objective.
- Determine what individuals or groups in the organization will be involved in the implementation of the plan. Then decide who will be responsible for what phases of the action plan.
- Identify the steps needed to accomplish the goal.
- Set the steps, flow procedure they need to accomplish the goal.

- Set a deadline for each step.
- Identify and set mechanism of evaluating action plan
- Evaluate the goals, action plan or the people doing them periodically to check their progress and make sure members are working to achieve them.
- Conduct an evaluation of the goals by the end of the year. From the evaluation, make recommendations for next.

Human Resources

In this section identify and describe required professional, experience and number of man power need to allocating properly in each operational level, on it identify and specify which team, section or department take action or responsible to perform strategies based on operation plan.

For example:

Strategy	Responsible body

Note: The responsible body may be individual, or a group e.g. a team, section or department.

Physical Resources

In this section describe determining physical asset needed to implement strategy in an aspect of operation planning. Planners must determine the amount funding required for purchasing, hiring or maintaining physical resources. The implementation of strategies and tasks within the Operational Plan is dependent on the availability of physical resources, so assign adequate and appropriate Physical resource. E.g. Physical resource required for administrative purposes, directly provide to implement strategy, and buildings etc.

Budget

In this section organization determine amount of budget needs, when allocating budget consider overall situation current and future market, duration of operational plan, and allocating its budget properly for the implementation of a strategy. E.g. pay salaries, purchase equipment, and undertake advertising and promotion e.tc.

Performance Indicators

In this section states the implementation performance metrics action it stands as standard or reference point to measure the actual result of strategies and make comparisons between desired results and actual results.

Implementation Time Table

In this section describes implementation period of strategic plan activities, operation level of each tasks when, who will take responsibility and done. For example:

Strategy the strategies and tasks to be achieved / completed	**Responsibilities** the individuals or group who have responsibility for each task strategy / task	**Timeframe** the timeline for which the strategies/tasks must be completed	**Budget** Assigned budget	**Resources** Resources Needed (financial, human, physical & other)

15. Guiding Principles

Name	**Risk based**
Statement	Cyber security policy, procedure, guidelines and plan development should be based on risk assessed.
Motivation	Developing cyber security policy, procedure, guideline and plan based on sound understanding of organization risk profile and requirements.
Implication	The cyber security policy, procedure, guideline and plan developed address the organization risks.
Name	**Contextualize**
Statement	Considering the circumstances which the document is created, its function, purpose, use, time and recipient.
Motivation	To develop a cyber-security policy, procedure, guideline and plan tailor to the organization.
Implication	The cyber security policy, procedure, guideline and plan will be easily applicable for the organization.
Name	**Cost effective**
Statement	The development of and implementation of cyber security policy, procedure, guideline, and plan will be cost effective.
Motivation	To develop and implement cyber security policy, procedure, guideline, and plan throughout the organization in a cost effective manner.
Implications	The cyber security policy, procedure, guideline, and plan develop and implement with the possible minimum cost.
Name	**Alignment**
Statement	Creates alignment whilst developing cyber security policy, procedure, guidelines and plan at organizational and national level.

Motivation	Enabling the organization cyber security policy, procedure, guidelines and plan align and integrate with the national related document and directives.
Implications	Creating an integrated and aligned cyber security policy, procedure, guidelines and plan at all levels.
Name	**Tipping point**
Statement	It serves as a tipping point for organization and cyber security policy developer to develop cyber security policy, procedure, guideline, and plan.
Motivation	Creating conducive cyber security policy, procedure, guideline and plan development platform for organizations and cyber security policy developers.
Implications	Organization and cyber security policy developers refer this methodology to develop cyber security policy, procedure, guidelines and plan document.

16.Assumptions

- Organization may consider other principles based on their organizational/business context, other than mentioned above.
- Organization can add or remove the requirements listed under the methodology part (policy, strategy, procedure, guideline and plan) based on organizational/business context.

  Organization can substitute the content of what is written in the template section of policy, procedure, guideline, plan and procedure by considering their organization/business context.

17. Conclusion

The afro mentioned Methodologies and Templates will help organizations make their own contextualized, in tuned with their respective mission, vision, policy and strategy cyber security policies, procedures, guidelines and plans, which in turn help achieve their goals and objectives through the implementation of such frameworks. And, also help organizations own the resulting by products.

18. Reference:

1. Critical Mass Cyber security Requirement Standard. INSA 2009 E.C
2. Information Security Policies and Procedures Development Framework for Government Agencies in Saudi Arabia.
3. Health Service Executive (HSE) Procedure for developing Policies, Procedures, Protocols and Guidelines.
4. Policy on the Production and Control of Policies, Procedures, Protocols and Guidelines. Sandwell and West Birmingham clinical commissioning Group.
5. SANS Institute InfoSec Reading Room. Information Security Policy - A Development Guide for Large and Small Companies
6. http://www.leoisaac.com/operations/index.htm
7. http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf

+251-11-371-71-14
Fax: +251-11-3-20-40-37
P.O.BOX: 124498
contact@insa.gov.et
www.facebook.com/INSA.ETHIOPIA
www.insa.gov.et
Addis Ababa
Ethiopia