This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the placeholder to the

Cybersecurity Awareness Program Template

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press "Ctrl" + "H" keys simultaneously.
- Enter "<organization name>" in the Find text box.
- Enter your organization's full name in the "Replace" text box.
- Click "More", and make sure "Match case" is ticked.
- Click "Replace All".
- Close the dialog box.

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated By	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose 4
Detailed Roles and Responsibilities 4
Selecting Awareness Content 6
Implementation 7
Post Implementation 8
Annex A 10
    Cybersecurity Awareness Assessment Questionnaire 10
Roles and Responsibilities 18
Update and Review 18
Compliance 18

Purpose

This document aims to define the main elements needed for building and maintaining a comprehensive cybersecurity awareness program, as part of the <organization name>'s overall cybersecurity program. This document is presented in a life-cycle approach, ranging from preparation, implementation, through post-implementation and evaluation of the program. This document also describes how to:

- Select awareness topics
- Implement awareness material
- Evaluate the effectiveness of the program

The requirements in this program are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to (ECC-1:2018) in addition to other related cybersecurity legal and regulatory requirements.

Scope

The scope of this document covers what <organization name> should do to develop, implement, and maintain a cybersecurity awareness program.

The cybersecurity awareness program is intended to help and educate several key audiences of the <organization name> including: Senior Management, Information Technology (IT) personnel, and all personnel (employees and contractors).

The success of <organization name>'s cybersecurity awareness program depends on the ability of these personnel to work toward a common goal of protecting <organization name>'s information and IT-related resources.

Detailed Roles and Responsibilities

1. <head of cybersecurity function>

<head of cybersecurity function> is tasked to oversee personnel with significant responsibilities for information security. <head of cybersecurity

function> should work with the <Learning and Development (L&D) function> of <organization name> to:

- Establish overall strategy for the cybersecurity awareness program.
- Ensure that the senior management, IT personnel and the leadership of <organization name> understand the concepts and strategy of the cybersecurity awareness program, and are informed of the progress of the program's implementation.
- Ensure that the cybersecurity awareness program of <organization name> is funded.
- Ensure the training of <organization name> personnel with significant security responsibilities.
- Ensure that effective tracking and reporting mechanisms are in place.
- Appoint the cybersecurity program manager who will be responsible for the implementation of the program.

2. Cybersecurity Program Manager

The cybersecurity program manager has tactical-level responsibility for the awareness program. In this role, the program manager should:

- Ensure that awareness material developed is relating to existing technologies and timely for the intended audiences.
- Ensure that awareness material is effectively deployed to reach the intended audience.
- Ensure that users and managers have an effective way to provide feedback on the awareness material and its presentation.
- Ensure that awareness material is reviewed periodically and updated when necessary.
- Assist in establishing a tracking and reporting strategy.

3. Management

Managers have responsibility for complying with cybersecurity awareness requirements established for their personnel. Management should:

- Work with the <head of cybersecurity function> and cybersecurity program manager to meet shared responsibilities.
- Serve in the role of system owner and/or data owner, where applicable.
- Consider developing individual development plans (IDPs) for users in roles with significant security responsibilities.

- Promote the professional development and certification of the cybersecurity program staff, and others with significant security responsibilities.
- Ensure that all users and contractors who manage and work on <organization name>'s systems (i.e., general support systems and major applications) are appropriately trained in how to fulfill their cybersecurity responsibilities before allowing them access.
- Ensure that users and contractors understand specific rules of each system and application they use.
- Work to reduce errors and omissions by users due to lack of awareness and/or training.

4. Personnel

Users are the largest audience in any organization and are the single most important group of people who can help to reduce unintentional errors and IT vulnerabilities. Users may include employees, contractors, visitors, guests, and other associates requiring access to <organization name>'s assets. Users must:

- Understand and comply with the security policies and procedures of <organization name>.
- Attend training to understand the rules of behavior for the systems and applications to which they have access.
- Work with management to meet training needs.
- Be aware of actions they can take to better protect the information of <organization name>.

Selecting Awareness Content

1. IT Personnel:

The cybersecurity awareness program must cover but not be limited to the following topics intended for IT Personnel:

- Asset Management
- Backup and Recovery
- Disaster Recovery
- Cryptography
- Hardening
- Identity and Access Management
- Patch Management

- Security Incident Management
- Vulnerability Management

2. Senior Management:

The cybersecurity awareness program must cover but not be limited to the following topics intended for senior management:

- Policies and Standards
- Cybersecurity Risks with focus on:
  - Threat Landscape and Cybersecurity Trends
  - Financial Impact
- System and Application Audits
- Regulatory and Legal Requirements
- Security Incident Management
- Enterprise Business Continuity

3. Personnel:

The cybersecurity awareness program must cover but not be limited to the following topics intended for employees and contractors:

- Security hygiene and common mistakes
- Cyber Security Policies:
  - Remote Working
  - Acceptable Use
  - Removable Media
  - Social Media Use
  - Internet and Email Use
  - Mobile Use
- Social Engineering Attacks
- Data Protection
- Password and Authentication
- Security at Home
- Public Wi-Fi Use

Implementation

The cybersecurity awareness program should be implemented only after:

- A strategy for designing and implementing the cybersecurity awareness program has been developed.

- An awareness program plan for implementing that strategy has been completed.
- Awareness material has been developed.
- Financial requirements must also be addressed.

1. Communicating the Plan

The program implementation must be fully explained to the <organization name>'s senior management to achieve support for its implementation and commitment of necessary resources. This is the explanation of the management and staff roles and responsibilities, as well as expected results of the program and benefits to <organization name>.

2. Delivering Awareness Material

Techniques for effectively delivering awareness material should take advantage of technology that supports the following features:

- Ease of use (e.g., easy to access and easy to update/maintain);
- Scalability (e.g., can be used for various audience sizes and in various locations);
- Accountability (e.g., capture and use statistics on degree of completion); and

Some of the more common techniques that the can be employed include:

- Interactive video training (IVT)
- Web-based training
- Non-web, computer-based
- Onsite, instructor-led awareness sessions
- Posters and Brochures
- Screen Savers and Desktop background

Blending various awareness delivery techniques in one session can be an effective way to present material and hold an audience's attention.

Post Implementation

The <cybersecurity function> of <organization name> must incorporate mechanisms into the cybersecurity strategy to ensure the cybersecurity awareness program continues to be relevant and compliant with overall objectives. Therefore, the program must pay attention to technology

advancements, IT infrastructure and organizational changes, and shifts in organizational mission and priorities. Continuous improvement is essential to the success of the cybersecurity awareness program.

1. Evaluation and Feedback

Formal evaluation and feedback mechanisms are critical components of any security awareness, training, and education program. Continuous improvement cannot occur without a good sense of how the existing program is working. In addition, the feedback mechanism must be designed to address objectives initially established for the program.

An evaluation assessment needs to be carried out, to identify the cybersecurity awareness and training related maturity level of <organization name>. For this purpose, <organization name> might use the example Cybersecurity Awareness Assessment Questionnaire (Annex A of this document).

A feedback strategy needs to incorporate elements that will address:

- Quality
- Scope
- Deployment method (e.g., web-based, onsite, offsite)
- Level of difficulty
- Ease of use, duration of session
- Relevancy
- Suggestions for modification

<organization name> must also do periodic testing to validate the effectiveness of the cybersecurity awareness program (i.e. simulated attacks, phishing campaign, etc.)

2. Program Success Factors

It is critical that everyone is capable and willing to carry out their assigned cybersecurity roles in <organization name>. Listed below are some key indicators to gauge the support for, and acceptance of, the program.

- Sufficient funding to implement the agreed-upon strategy.
- Clearly defined roles and responsibilities to effectively implement the strategy.
- Executive/Senior Management support

- Use of metrics
- Level of attendance at mandatory cybersecurity trainings.

Annex A

Cybersecurity Awareness Assessment Questionnaire

Building Cybersecurity Awareness	
Initiatives	
1	Has <organization name> recognized the need for awareness of cybersecurity threats and vulnerabilities?
Answer	Comments
2	Is the awareness of cybersecurity threats and vulnerabilities only at initial stages of discussion at <organization name>?
Answer	Comments
3	Has <organization name> taken into consideration the involvement of relevant stakeholders while developing the Cybersecurity Awareness Program?
Answer	Comments
4	Are the adequate resources available at <organization name> for the implementation of a Cybersecurity Awareness Program?
Answer	Comments

5	Does <organization name> have a detailed implementation plan published for the Cybersecurity Awareness Program?
Answer	Comments
6	Has <organization name> developed a Cybersecurity Awareness Program?
Answer	Comments
7	Is the Cybersecurity Awareness Program co-ordinated at <organization name>?
Answer	Comments
8	Is the initial system of mechanisms and metrics available to review the Cybersecurity Awareness Program at <organization name>?
Answer	Comments
9	Are there assigned personnel with sufficient authority and resources to deliver the actions of the Cybersecurity Awareness Program at <organization name>?

Answer	Comments
10	Does <organization name> have cybersecurity awareness portal to improve cybersecurity skills and knowledge?
Answer	Comments
11	Does <organization name> take part in third-party awareness-raising programs, courses, seminars and online resources?
Answer	Comments
12	Does <organization name> have Cybersecurity Awareness Program review processes and outcome-oriented metrics are in place?
Answer	Comments
Executive Awareness Raising	
13	Is awareness raising on cybersecurity issues for executives existent at <organization name>?
Answer	Comments

14	Are executives aware of their responsibilities to shareholders, customers, and employees in relation to cybersecurity at <organization name>?
Answer	Comments
15	Are the executives made aware of general cybersecurity issues, that might affect their <organization name>?
Answer	Comments
16	Are the executives know how these issues and threats might affect <organization name>?
Answer	Comments
17	Are the executives of particular departments of <organization name> (e.g., finance and telecommunications) have been made aware of cybersecurity risks in general, and how the organization deals with cybersecurity issues?
Answer	Comments

18	Are the executives of particular departments of <organization name> (e.g., finance and telecommunications) has been made aware of the strategic implications of the cybersecurity risks?
Answer	Comments
19	Does <organization name>'s Cybersecurity Awareness Program of executives address cybersecurity risks in general (e.g., primary methods of attack, how the organization deals with cyber issues)?
Answer	Comments
Awareness and Training Policy	
Initiatives	
20	Are there cybersecurity educators available at <organization name>?
Answer	Comments
21	Are there qualification programs for educators at <organization name>?
Answer	Comments

22	Are there computer science courses offered that may have a security component at <organization name>>?
Answer	Comments
23	Are there cybersecurity-related courses offered to the employee at <organization name>?
Answer	Comments
24	Are there qualification programs for cybersecurity educators being explored by existing qualified educators at <organization name>?
Answer	Comments
25	Are there any third-party educational courses available in cybersecurity-related fields (e.g., information security, network security, cryptography) at <organization name>?
Answer	Comments
Awareness and Training Policy	
Initiatives	
26	Does any training programs in cybersecurity exist at <organization name>?

Answer	Comments
27	Is training provided for <organization name>'s general IT staff on cybersecurity issues so that they can react to incidents as they occur?
Answer	Comments
28	Is training provided for <organization name>'s dedicated security professionals on cybersecurity issues so that they can react to incidents as they occur?
Answer	Comments
29	Are there any cybersecurity related professional certifications provided by <organization name> for their employees?
Answer	Comments
30	Are the cybersecurity training programs structured at <organization name>?
Answer	Comments

31	Are there any national or international cybersecurity frameworks and international best practices are taken into consideration when designing professional training courses?
Answer	Comments
32	Are the cybersecurity related needs of <organization name> well understood (e.g., list of training requirements is documented)?
Answer	Comments
33	Are cybersecurity training programs are recognized and offered in general for employee?
Answer	Comments
Uptake	
34	Is the cybersecurity knowledge transferred from trained employees to untrained employees at <organization name>?
Answer	Comments

Roles and Responsibilities

1- **Program Owner:** <head of the cybersecurity function>
2- **Program Review and Update:** <cybersecurity function>
3- **Program Implementation and Execution:** <information technology function>
4- **Program Compliance Measurement:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the program at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- The <head of the cybersecurity function> will ensure compliance of <organization name> with this program on a regular basis.
2- All personnel at <organization name> must comply with this program.
3- Any violation of this program may be subject to disciplinary action according to <organization name>'s procedures.